MARKAZ ALKHEBRAH
المركز الدولي للخبرة الاستشاري
www.consulting-marrakech.com

المؤتمر العلمي الدولي تحت عنوان:

الأمن السيبراني في تشريعات الدول العربية

المنعقد يومي: الجمعة والسبت 16 و17 يوليوز 2021
بنادي المحامين تاركة مراكش

بسم الله الرحمن الرحيم



INTERNATIONAL
Scientific Indexing

Fresh Ideas for Growing your Citations

Certificate

This is to certify that مجلـة القـانون والأعمـال is indexed in International Scientific Indexing (ISI). The Journal has Impact Factor Value of **0.821** based on International Citation Report (ICR) for the year **2018-19**. The URL for journal on our server is https://isindexing.com/isi/journaldetails.php?id=8854

Editor ICR Team
(ISI)

International Scientific Indexing
(ISI)



شهادة رقم (481-2020)

معامل التأثير العربي

مجلة القانون والأعمال الدولية

ISSN:2509-0291

قد حصلت على معامل التأثير العربي لعام 2019 وقدرة 0.6

الاستاذ الدكتور محمود عبد العاطي



مدير مشروع معامل التأثير العربي
13 أكتوبر 2019 م

اللجة التنسيقية للمؤتمر

الدكتور: ضياء نعمان – النقيب: محمد الحميدي – الأستاذ: أيوب بوحود – الأستاذ: الجيلالي الحمومي – الأستاذة: زهرة نسيم الصباح – الدكتور: ثاني بن علي آل ثاني – الدكتور: مازن المعشري – الدكتور: رياض فخري – الدكتور: نور الدين الناصري – الدكتور: طارق مصدق – الأستاذ: عبد الرحيم الجمل – الدكتور: عمر الخطايبة – الأستاذ: محمد رافع – الدكتور: عبد الباسط محمد سيف الحكيمي – الأستاذ: مبارك السليطي.

اللجنة العلمية للمؤتمر

الدكتور: عبد الرحيم بنبوعيدة – النقيب: محمد الحميدي – الدكتور: مصطفى مالك – الدكتور: محمد مومن – الدكتورة: الهام العلمي – الدكتورة: لطيفة قبيش – الدكتورة: أمينة عتيوي – الدكتور: حسن زرداني – الدكتور: يحيى علوي – الدكتورة: نجاة العماري.

اللجنة المنظمة للمؤتمر

الأستاذ: أيوب بوحدو – الدكتور: حسن زرداني - الدكتور: أنس الطالبي – الأستاذة: سهام البدراوي – الأستاذة: دنيا الغولاط - الأستاذ: هشام موهوب - الأستاذة: كحواش نزهة - الأستاذ: بدر صبور - الأستاذة: رشيدة المنعيم - الأستاذ: عبد الخالق الحرفاوي - الأستاذ: زهير الرزقي.

لجنة التواصل والعلاقات الخارجية للمؤتمر

الدكتور: مصطفى الفوركي - الدكتور: عالي الطوير - الدكتور: سعد بهيتي - الدكتور: الحبيب بداع – الأستاذة: نرمين نعمان – الأستاذ: محمد بو ليلي.

لجنة صياغة البيان الختامي للمؤتمر

الأستاذ: الجيلالي الحمومي - الأستاذ: أيوب بوحدو - الأستاذة: زهرة نسيم الصباح - الأستاذ: الراجي الحسين - الأستاذة: خديجة فاروق - الأستاذة: كحواش نزهة - الأستاذ: القالبة عبد الكريم.

لجنة التواصل والمراجعة

الطالب الباحث مصطفى سكيليس - الطالب الباحث عبد الرحمان الغزالي - الطالب الباحث عبد العزيز بولحرير - الطالب الباحث أشرف معلومي - الطالب الباحث وصال الخير - الطالبة الباحثة صفاء خبان - الطالبة الباحثة أسماء نوعم - الطالبة الباحثة عائشة رزوقي - الطالب الباحث مرشد اليزيد – الطالب الباحث عبد الواحد السملالي.

التصوير والتقنيات والنقل الخارجي

الأستاذ: أنس عبودي

الاشراف الفني

الأستاذ: محمد أمين اسماعيلي

محتويات العدد

الجلسة العلمية الثانية

الجلسة العلمية الثالثة

الجلسة العلمية الرابع

الجلسة العلمية الخامسة

الجلسة العلمية السادسة

الجلسة الافتتاحية

كلمة الأستاذ ضياء نعمان

كلمة اللجنة التنسيقية

للمؤتمر العلمي الدولي للأمن السيبراني في تشريعات الدول العربية

رئيس المركز الدولي للخبرة الاستشاري

تعتبر الأبحاث المنشورة للمؤتمرات العلمية بمثابة العمود الفقري لتقدم البحث العلمي وملجأ للأشخاص المهتمين بأخر المستجدات في مجال الحقول المعرفية ، مما حذا بالجهات المنظمة للمؤتمر العلمي الدولي للأمن السيبراني في تشريعات الدول العربية القيام بنشر أبحاث المؤتمر وبالتعاون مع مجلة القانون والأعمال الدولية.

ونظرا لأهمية موضوع المؤتمر حيث نعيش اليوم ثورة معرفية بسبب التقدم العلمي والتكنولوجي وخصوصا ما تولد عنها من تطور في مجال الاتصال الكوني، حيث يسهل على كل مدقق أن يلاحظ ويتابع التحول الكيفي الذي حدث في مجال توليد المعلومات، وتداولها على المستوى العالمي، حيث بزغ فجر جديد هو فجر مجتمع المعلومات وترتب على نشوئه وتطوره آثار كبرى في مجال التزاحم المعرفي من ناحية والاتصال بين البشر من ناحية أخرى، حيث تحتل المعلومات مكانة متميزة في عصرنا الحالي، وهي محور كل مناقشة تتعلق بالمعلوماتية بوصفها علم معالجة المعلومات، كما أن محترفي المعلومات يحتلون مكانة متميزة في المجتمعات الصناعية والتي تحكمها التقنيات الحديثة.

ولعل أبرز الظواهر لمجتمع المعلومات الكوني في الوقت الحاضر هو ظهور شبكة الإنترنت التي تقوم على استخدام الحواسب الآلية المرتبطة ببعضها عالميا مما سيؤدي إلى تحسين وسائل تبادل المعلومات، فالإنترنت حلقة وصل بالشبكة العنكبوتية الدولية والتي تربط ملايين مصادر المعلومات في شبكة واحدة.

ولأن الشبكة العالمية للمعلومات لها مواصفات تقنية وفنية خاصة، تؤسس لمخاطر معينة، فإن اتصال الشبكات بها، يعرض هذه الأخيرة لمخاطر معينة. وبذلك، يمكن تصور تعرض النظام لاعتداء،

يجعله يتوقف عن تأدية الخدمات التي كان يقدمها، أو يجعله يعرض أسرار المؤسسات والأفراد، سواء الشخصية منها أو الصناعية والمهنية، أو بما يؤدي إلى تلف البيانات الحساسة، أو بث معلومات مغلوطة.

لهذا، فإن الأمن السيبراني يرتكز على تعزيز الحماية الناجمة عن تدابير الحد من مخاطر التكنولوجيا الرقمية، بسبب استخدامها المتزايد للأغراض غير القانونية، كما يرتكز على العمليات القائمة على ضمان سرية وسلامات المعلومات والبيانات من كل الهجمات الرقمية.

وقد شاع استخدام مصطلح الأمن السيبراني في نطاق أنشطة معالجة ونقل البيانات بواسطة أنظمة الحاسب الآلي، على الرغم من ظهور الحاجة إليه قبل استحداث وسائل التكنولوجيا الحديثة للمعلومات، وباستبدال الطرق التقليدية لحفظ وتخزين ومعالجة المعلومات بالطرق الرقمية الحديثة، أصبحت تلك المعلومات مهددة أكثر مما كانت عليه في السابق، بحيث يسهل الوصول إليها أكثر من ذي قبل، وبذلك أصبحت الحاجة إلى أمن المعلومات أساسية، وباتت هاجسا يؤرق العديد من الجهات.

لذا يمكن القول، أن العصر الرقمي له إفرازات سلبية، تشكل مخاطر يتم العمل على التصدي لها بجهود تنجح أحيانا وتخفق أحيانا أخرى، ومن أكبر سلبيات هذا العصر هو عدم تحقيق الأمن السيبراني، حيث استدعى الأمر بناء جوانب قانونية لحماية المعلومات من طرف التشريعات العربية من أجل تحقيق هذا الأمن وبيان المخاطر التي تهدد المعلومات ومصادرها وآليات ووسائل وأدوات الحماية التقنية لها واستراتيجياتها.

ونظرا لهذه الأسباب نظم كل من المركز الدولي للخبرة الاستشاري، وهيئة المحامين بمراكش، والمكتب الجهوي للودادية الحسنية للقضاة بدائرة محكمة الاستئناف بمراكش، ومختبر البحث قانون الأعمال، كلية العلوم القانونية والسياسية جامعة الحسن الأول بسطات، وماستر العلوم الجنائية والأمنية، كلية العلوم القانونية والاقتصادية والاجتماعية جامعة القاضي عياض بمركش، وماستر المعاملات الالكترونية، كلية العلوم القانونية والسياسية جامعة الحسن الأول بسطات، ومجلة القانون والإعمال الدولية، المؤتمر العلمي الدولي، الأمن السيبراني في تشريعات الدول العربية، والذي انعقد يومي الجمعة والسبت 16و17 يوليوز2021 ، بنادي المحامين تاركة مراكش.

حيث كانت أهداف المؤتمر تتمثل في :

- تعزيز دور البحث العلمي في مجال الأمن السيبراني.

- تسليط الضوء على التوجهات الإستراتيجية في تشريعات الدول العربية في مجال الأمن السيبراني.

- إبراز ايجابيات وسلبيات تشريعات الأمن السيبراني في الدول العربية.

- معرفة الرؤية النظرية المطروحة للأمن السيبراني.

- معرفة الدور الذي يقوم به الأمن السيبراني في التنمية الاقتصادية والاجتماعية.

وقد طرح المؤتمر على جميع الباحثين المهتمين بموضوعه مجموعة من المحاور تتمثل في: استراتيجيات الأمن السيبراني في تشريعات الدول العربية ، واقع السياسات الدولية للأمن السيبراني، المؤسسات الفاعلة في تشريعات الأمن السيبراني في تشريعات الدول العربية، الأمن السيبراني والإعلام عبر الوسائط الالكترونية، الأمن السيبراني والجرائم المرتكبة عبر الوسائط الالكترونية، الأمن السيبراني والتجارة عبر الوسائط الالكترونية، الأمن السيبراني في مجال العدالة، الأمن السيبراني والقضايا الاجتماعية والأخلاقية، الأمن السيبراني وسلامة المعطيات ذات الطابع الشخصي، الأمن السيبراني وامن نظم المعلومات، الأمن السيبراني ومقدمي الخدمات الرقمية، الأمن السيبراني وامن الاتصالات، الأمن السيبراني والإدارة الرقمية، الأمن السيبراني ومواقع شبكات التواصل الاجتماعي.

وبناء على ذلك كانت الاستجابة للمشاركة في المؤتمر جد واسعة من طرف باحثين ومهتمين وخبراء في مجال الأمن السيبراني من عدة دول وهي المغرب، اليمن، مصر، قطر ، الأردن، الجزائر، موريتانيا ، ليبيا، السودان، سلطنة عمان، الإمارات، البحرين، العراق، بريطانيا.

وقد تكونت جلسات المؤتمر من جلسة افتتاحية وسبع جلسات علمية وجلسة ختامية على مدار يومين، عرفت تقديم 37 مداخلة (33 مداخلة من أصل 37 كانت مقررة) عبر مساحة زمنية قدرها 16 ساعة و30 دقيقة.

وقد اندرج هذا المؤتمر ضمن الجهود المشتركة لمختلف الشركاء والمتدخلين من اجل تشخيص الأوضاع المستجدة في المجالات المعرفية المتنوعة في ظل التطورات التكنولوجية والرقمية المتسارعة ، وكيفية تحقيق الأمن السيراني .

وعرف المؤتمر حضورا نوعيا متميزا سواء من زاوية الفئة أو من زاوية مقاربة النوع، حيث سجلت لوائح الحضور مشاركة واسعة للشباب بنسبة فاقت 80 بالمئة، كما سجلت مشاركة نسائية مهمة محددة في 40 بالمائة.

وعلى مستوى الخريطة المهنية فقد شهد المؤتمر حضور مشاركين من مختلف القطاعات المهنية وخاصة الجامعية منها (أساتذة وطلبة باحثين) وكذلك من هيئة الدفاع(محامين رسميين ومتمرنين) ومن أسرة القضاء بشقيه الجالس والواقف، فضلا عن ممثلين لجمعيات ومنظمات المجتمع المدني والحقوقي ، ووسائل الإعلام المسموعة والمرئية والمكتوبة.

و قد شكل المؤتمر مناسبة للتعرف على الأوضاع القانونية للأمن السيبراني في الدول العربية المشاركة. كما أنه كان مناسبة لفتح نقاش جاد ومسؤول من خلال تفاعل المشاركين مع المتدخلين بشأن ما أثير من مواضيع ذات الصلة بالأمن السيبراني.

عن اللجنة التنسيقية للمؤتمر

الدكتور: ضياء نعمان

كلمة الأستاذ النقيب محمد الحميدي

نقيب هيئة المحامين بمراكش

-السادة النقباء

-السادة المسؤولون القضائيون

-السيد عميد كلية العلوم القانونية والاقتصادية والاجتماعية جامعة القاضي عياض بمراكش

-السيد رئيس المكتب الجهوي للودادية الحسنية للقضاة بدائرة محكمة الاستئناف بمراكش.

-السيد رئيس المكتب الجهوي لنادي القضاة بمراكش.

-السيد رئيس المركز الدولي للخبرة الاستشاري

-السيد منسق ماستر العلوم الجنائية والامنية بكلية العلوم القانونية والاقتصادية والاجتماعية جامعة القاضي عياض بمراكش

-السيد ممثل مختبر البحث قانون الاعمال كلية العلوم القانونية والسياسية جامعة الحسن الثاني سطات.

- السيد منسق ماستر المعاملات الالكترونية كلية العلوم القانونية والسياسية جامعة الحسن الاول بسطات.

-السيد مدير المركز الدولي للخبرة الاستشاري.

-السيد مدير مجلة القانون والاعمال الدولية.

- السدة ممثلي الاعلام والمجتمع المدني.

- زميلاتي زملائي.

- حضرات السيدات والسادة ، الحضور الكريم كل باسمـــه وصفتــه والاحترام الواجب له،

مساء الخير للجميع.

يسعدنا بهيئة المحامين بمراكش أن نستضيف في هذا الفضاء أشغال المؤتمر الدولي حول موضوع: "**الأمن السيبراني في تشريعات الدول العربية**".

الموضوع في غاية من الأهمية خصوصا أن المغرب اليوم وكباقي الدول العربية ودول العالم يعيش ثورة في المجال الإلكتروني والتكنولوجي والمعلوميات، وظهور شبكة الانترنيت تعد من أبرز الظواهر في العالم المعلوماتي، بحيث أن الأنترنيت تعد حلقة وصل بالشبكة العنكبوتية الدولية والتي تربط ملايين مصادر المعلومات في شبكة واحدة، كما أنها جعلت اليوم العالم قرية صغيرة.

ولأن الشبكة العالمية للمعلومات لها مواصفات تقنية وفنية خاصة، تؤسس لمخاطر معينة، فإن اتصال الشبكات بها، يعرض هذه الأخيرة لمخاطر معينة وبذلك يمكن تصور تعرض النظام لاعتداء يجعله يتوقف عن تأدية الخدمات التي يقدمها أو يجعله يعرض أسرار المؤسسات والأفراد وأيضا أسرار الدول إلى مخاطر عديدة بشكل قد يؤدي إلى تلف البيانات الحساسة أو بث معلومات مغلوطة.

فالأمن السيبراني يرتكز على تعزيز الحماية الناجمة عن تدابير الحد من مخاطر التكنولوجيا الرقمية والتهديدات التي تمس بالخصوص بالأمن السيبراني للدول ، وهذه التهديدات تتمثل بصفة عامة في : التجسس السيبراني- الارهاب السيبراني- الحروب السيبرانية.

والمغرب يتجه نحو تعزيز أمنه المعلوماتي، بإقرار قانون جديد وهو القانون رقم 05.20 المتعلق بالأمن السيبراني، الصادر بتاريخ 25 يوليوز 2020 ، هذا القانون الذي يهدف إلى تعزيز أمن أنظمة المعلومات في إدارات الدولة والمؤسسات الرسمية وشركات الاتصال وتعزيز الثقة ودعم الاقتصاد الرقمي وبشكل أوسع ضمان استمرارية الأنشطة الاقتصادية والاجتماعية.

ويحدد هذا القانون قواعد ومقتضيات الأمن المطبقة على نظم معلومات إدارات الدولة والجماعات والمؤسسات والمقاولات الرسمية، وقواعد ومقتضيات الأمن المطبقة على البنيات التحتية ذات الأهمية الحيوية، وقواعد ومقتضيات الأمن المطبقة على مستغلي الشبكات العامة للمواصلات ومزودي خدمات الانترنيت.

ويأتي هذا القانون وعيا من الدولة بخطورة الهجومات الإلكترونية التي قد تستهدف نظم المعلومات وتمس الوظائف الحيوية للمجتمع أو الصحة أو السلامة أو الأمن أو التقدم الاقتصادي أو الاجتماعي وهو ما يفرض تعزيز الجهود لتحصين الأمن المعلوماتي للمملكة.

ويعرف النص "**الأمن السيبراني**" بكونه مجموعة من التدابير والإجراءات ومفاهيم الأمن وطرق إدارة المخاطر والتكوينات وأفضل الممارسات والتكنولوجيا التي تسمح لنظام معلومات بأن يقاوم أحداثا مرتبطة بالفضاء السيبراني من أن تمس بتوافر وسلامة وسرية المعطيات المخزنة أو المعالجة أو المرسلة.

وبموجب هذا القانون سيتم إحداث لجنة استراتيجية للأمن السيبراني ولجنة تابعة لها لإدارة الأزمات والأحداث السيبرانية الجسيمة، إضافة إلى السلطة الوطنية للأمن السيبراني، هذه اللجنة سيعهد إليها إعداد التوجهات الاستراتيجية للدولة في هذا المجال والسهر على ضمان صمود نظم معلومات الهيئات والبنيات التحتية ذات الأهمية الحيوية.

وهنا تجب الإشارة إلى أنه من أجل تسهيل عمل هذه اللجنة والتطبيق السليم للقانون المذكور يتعين على مستغلي الشبكات العامة للمواصلات ومزودي خدمات الأنترنيت ومقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية الاستجابة لطلبات هذه اللجنة المتعلقة بالدعم والمساعدة التقنية والتزويد بالمعلومات اللازمة.

كما يجب تأهيل جميع الفاعلين في هذا المجال وكذا ضباط الشرطة القضائية للبحث عن المخالفات لأحكام هذا القانون.

والمؤتمر المنعقد اليوم سيسلط الضوء على العديد من المعطيات بخصوص الأمن السيبراني في المغرب وفي التشريعات العربية من خلال مناقشة استراتيجة الأمن السيبراني في تشريعات الدول العربية، والتطرق لواقع السياسات الدولية للأمن السيبراني، ومناقشة الأمن السيبراني والإعلام والتجارة والعدالة عبر الوسائط الالكترونية، الأمن السيبراني والجرائم المرتكبة عبر الوسائط الالكترونية، وأيضا الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي وغيرها من المحاور التي سيتم عرضها ومناقشتها خلال مؤتمرنا هذا.

لن أطيل، متمنياتي لكم بنجاح أشغال هذا المؤتمر، ومتمنيات صادقة بأن يكون للمؤتمر الحالي مخرجات قوية وتوصيات يمكن من خلالها العمل على تنزيل وتفعيل المقتضيات القانونية على أرض الواقـــع.

وأجدد الترحاب والشكر للحضور الكريم.

كلمة الأستاذ عبد الرحيم الجمل

رئيس المكتب الجهوي للودادية الحسنية للقضاة

بدائرة محكمة الاستئناف بمراكش

الحمد لله والصلاة والسلام على رسول الله و آله وصحبه.

تحية طيبة ملؤها الود والتقدير والاحترام للحضور الكريم كل باسمه وصفته وما يجب له من تقدير واعتبار تليها أسمى عبارات الشكر والثناء والامتنان لكل المشاركين في تنظيم هذا المؤتمر العلمي المتميز وأخص بالشكر المركز الدولي للخبرة الاستشاري في شخص الأستاذ ضياء نعمان كما أشكر هيئة المحامين بمراكش وعلى رأسها السيد النقيب الأستاذ محمد الحميدي كما أشكر الأستاذ أيوب بوحدو الذي أخذ المبادرة وعرض علينا المشاركة في هذا الحفل العلمي البهيج والشكر موصول لزملائي القضاة الذين لبوا الدعوة وعبروا عن استعدادهم للإسهام بمداخلاتهم في هذا المؤتمر المبارك.

إن الودادية الحسنية باعتبارها أول جمعية مهنية مغربية للقضاة تنشط في عدة مجالات تهم الحياة المهنية والاجتماعية للسادة القضاة تعتبر الحقل العلمي والنقاشات القانونية الهادفة والموضوعية من أهم المحاور التي تركز عليها أنشطتها لما فيها من فائدة وتكوين مستمر وتبادل للأفكار والآراء فمهنة القضاء تتطلب المواكبة وتحيين المعلومة ومسايرة تطورات العصر التي أصبحت تسير بسرعة عالية تحتم علينا السير بسرعتها وإلا صرنا متخلفين عن الركب وهو ما يتنافى وطموح المملكة المغربية تحت القيادة الرشيدة لجلالة الملك محمد السادس الذي جعل من المغرب دولة صاعدة تأخذ طريقها بثبات نحو نادي الكبار ولعل ما عاشه العالم خلال السنة الماضية والسنة الحالية من تفشي وباء كوفيد 19 قد أبان على أن المغرب من الدول الأولى في العالم التي تعاملت بطريقة علمية وبحنكة عالية في تدبير هذه الأزمة الصحية التي كانت لها تداعيات اقتصادية واجتماعية خطيرة ومن بين الأمور التي نجحت فيها بلادنا خلال هذه الأزمة استعمالها لوسائل التواصل عن بعد ومجال الانترنيت أو ما يسمى بالمجال السيبراني

هذا المجال الحي المتميز بدينامية عالية والذي يصعب التحكم فيه لأنه لا هو بالمجال الطبيعي ولا الجغرافي فهو غير اقليمي يطغى عليه طابع العولمة والمنافسة والصراع مما يجعله مجالا استراتيجيا هاما ولعل العدد الهائل لمستعملي شبكة الأنترنيت الذي بلغ 4 ملايير وخمسمائة وأربعين مليون شخص عبر العالم سنة 2020 و عدد مستعملي شبكة التواصل الاجتماعي الذي بلغ 3 ملايير وثمانمائة مليون شخص ليعبر عن ضخامة هذا المجال واتساع رقعته.

ومن خلال ما سبق تتبين أهمية موضوع المؤتمر وهو الأمن السيبراني في التشريعات العربية فقد أصبح العالم يستعمل المجال السيبراني بكثرة وفي جميع مناحي الحياة وفي أمور خاصة ودقيقة تتميز بطابع الشخصية والسرية في أغلب الأحيان ويستعمله الأفراد والجماعات والأشخاص الذاتيين كما الأشخاص المعنويين بل تستعمله الدول ضد بعضها البعض فيما أصبح يعرف بالحرب السيبرانية فهو خزان ضخم لمجموعة من المعلومات العامة والخاصة والشخصية والمالية والسرية ... الخ مما جعله عرضة للكثير من التهديدات فقد أصبح يتعرض للقرصنة والاختراق والسرقة مما يستدعي أولا وقبل إطلاق إستراتيجية عامة للأمن السيبراني معرفة التهديدات الحقيقية التي يتعرض لها هذا المجال لذلك فإن المتدخلين في هذا المؤتمر العلمي الكبير مطالبين بالجواب على مجموعة من التساؤلات من قبيل ماذا أعدت التشريعات العربية ومن بينها المغرب من قوانين لتنظيم هذا المجال وحمايته و هل يمكن تعريف وتحديد التهديدات الحقيقية التي يتعرض لها المجال السيبراني ثم ما مدى إمكانية وضع قواعد يحترمها الجميع لتنظيم عالم هو في الأصل مجزء وكيفية التوفيق بين مبدأ سيادة الدول وقواعد تنظيم هذا المجال إلى غير ذلك من الأسئلة والاشاكاليات التي سيتناولها السادة المتدخلين خلال هذين اليومين وإنني جد متفائل لنتائج هذا المؤتمر نظرا لقامة وكفاءة السادة المتدخلين متمنيا لهم التوفيق والسداد ولأعمالنا النجاح و الفلاح وقل اعملوا فسيرى الله عملكم ورسوله والمومنون والسلام عليكم ورحمة الله تعالى وبركاته .

كلمة الدكتور عبدالرحيم بن بوعيدة

أستاذ التعليم العالي، منسق ماستر العلوم الجنائية والأمنية، كلية العلوم القانونية والاقتصادية والاجتماعية

جامعة القاضي عياض مراكش

- السيد رئيس المركز الدولي للخبرة الاستشاري.
- السيد نقيب هيئة المحامين بمراكش.
- السيد عميد كلية العلوم القانونية والاقتصادية والاجتماعية جامعة القاضي عياض مراكش.
- السيد رئيس المكتب الجهوي للودادية الحسنية للقضاة بدائرة محكمة الاستئناف بمراكش.
- السيد رئيس المكتب الجهوي لنادي قضاة المغرب بمراكش
- السيد مدير مختبر البحث قانون الأعمال، كلية العلوم القانونية والسياسية جامعة الحسن الأول بسطات.
- السيد منسق ماستر المعاملات الالكترونية، بكلية العلوم القانونية والسياسية جامعة الحسن الأول بسطات.
- السيد مدير مجلة القانون والإعمال الدولية.

السيدات والسادة الحضور:

إن ماستر العلوم الجنائية والأمنية وفي إطار سياسة الانفتاح الذي نهجها في مجال البحث العلمي فإنه يشارك اليوم مع شركائه في تنظيم هذا المؤتمر وهي ليست الأولى في هذا المجال ، فقد سبق له أن شارك في العديد من المؤتمرات الدولية تخص الفضاء السيبراني.كما أنه من أول الماسترات التي تدرس العديد من المواد في هذا المجال.

الحضور الكريم:

يأتي سياق انعقد هذا المؤتمر في وقت أصبح الأمن السيبراني ضرورة ملحة من أجل تأمين مجال الشبكات والاتصالات، والدليل على ذلك أن اغلب الدول بادرت إلى إصدار قوانين خاصة لتنظيمه، ومن هذه الدول المغرب عن طريق إصدار القانون رقم 05.20 المتعلق بالأمن السيبراني.

ونظرا لأن الأمن السيبراني ذو بعد دولي، فقد جاء انعقاد هذا المؤتمر لمعرفة التوجهات الإستراتيجية والرؤية النظرية المطروحة في تشريعات العديد من الدول المشاركة وهي المملكة المغربية، اليمن، الجزائر،،قطر، موريتانيا، ليبيا، مصر،الأردن، السودان ،سلطنة عمان، الإمارات العربية المتحدة، العراق، مملكة البحرين،وبريطانيا.

السيدات والسادة الحضور:

إن ماستر العلوم الجنائية والأمنية بكلية العلوم القانونية ولاقتصادية والاجتماعية جامعة القاضي عياض مراكش، له عظيم الشرف للمشاركة في أشغال هذا المؤتمر بجانب كل من المركز الدولي للخبرة الاستشاري، وهيئة المحامين بمراكش، والمكتب الجهوي للودادية الحسنية للقضاة بدائرة محكمة الاستئناف بمراكش، والمكتب الجهوي لنادي قضاة المغرب بمراكش، ومختبر البحث قانون الأعمال، كلية العلوم القانونية والسياسية جامعة الحسن الأول بسطات، وماستر المعاملات الالكترونية، بكلية العلوم القانونية والسياسية جامعة الحسن الأول بسطات، ومجلة القانون والإعمال الدولية.

وفي الأخير نتقدم بالشكر الجزيل إلى جميع السيدات والسادة المتدخلين ونسأل الله التوفيق والسداد.

والسلام عليكم ورحمة الله وبركاته

كلمة الأستاذ محمد رافع

رئيس المكتب الجهوي لنادي قضاة المغرب بمراكش

يعرف العالم اليوم ثورة تكنولوجية ومعرفية هامة ساهم فيها تطور العلم والتكنولوجيا، حيث أصبح العالم قرية صغيرة بسبب وسائل التواصل التي مكنت من تجاوز عقبة البعد الجغرافي بين الدول والشعوب، كما سهل مكنة الحصول على جميع المعلومات بكافة أنواعها وأشكالها بمجرد الضغط على الزر أو تحريك الشاشة وتفعيل محركات البحث، إلا أن ذلك ورغم إيجابياته الكبرى، ومنافعه العظمى لم يكن ليسلم كشأن كل شيء يحمل في طياته نعما ونقما، لاسيما إذا فوجئنا بكون المعلومة أصبحت تحتل مركز الصدارة في الوقت الراهن لكون أصحاب المعلومات هم من يتبوأ محور الاهتمام في المجتمعات المتقدمة التي تسمو بتوفرها على أحدث التقنيات.

وارتباطا بما ذكر ظهر للعلن مصطلح الأمن السيبراني في مجال معالجة ونقل البيانات بواسطة الأنظمة المعلوماتية تزامنا مع تغير الطرق القديمة في حفظ واستثمار المعلومات بالطرق الرقمية العصرية التي أصبحت عرضة للخطر والقرصنة وسوء الإستعمال، وهو ما حتم وجود أمن لهاته المعلومات سواء على المستوى الأمني أو التجاري أو الصناعي أو المعرفي إلى غير ذلك من المجالات التي سيتطرق المؤتمر من خلال المواضيع التي أحاطت بالظاهرة في محاولة لسبر أغوارها، وهو ما شكل هاجسا مؤرقا للجهات المشرفة على حفظ هاته المعلومات والحيلولة دون الوصول إليها.

وكما أن للثورة الرقمية منافع ومصالح لا حد لها، ويتم اكتشاف مزاياها يوما بعد يوم، فإن لها كذلك نتائج سلبية وعواقب وخيمة إن لم يتم التصدي لها، ولهذا سارعت مجموعة من الدول ولا سيما العربية باعتبار أهميتها في هذا المؤتمر إلى سن تشريعات لمحاولة تحقيق الأمن وكشف المخاطر التي تحدق بمجال المعلومات ومصادرها وآليات وسبل الحماية المعلوماتية وطرق وبرامج معالجتها، ومن هذا المنطلق أصبح الأمن السيبراني قطب الرحى في السياسات الأمنية والإقتصادية للحفاظ على أمن المجتمع برمته وحماية خصوصيات الأشخاص والأسر والعائلات باعتبارهم أسس الدول وأعمدتها،

ومصدر قوة وتآزر المجتمع والحفاظ على بنيانه من الظواهر الإجرامية التي غزت كل الميادين التي تتداول من خلالها الأموال والبضائع والأنماط الاجتماعية.

وقد دفعت هذه الظاهرة وغيرها المشرع في الدول العربية عموما وفي مغربنا الحبيب خصوصا، إلى دق باب السلطة التشريعية لمواكبة هذا التحدي وركوب هذه المغامرة لوضع تشريع يخاطب أناسا غير أولئك الذين كان يخاطبهم تشريعنا سابقامن حيث تكوينهم ونوعهم أو الأساليب الإجرامية التي يأتونها، حيث فرض الأمر على السلطة التشريعية أن تضاعف سرعتها وجهودها لمحاولة كبح جماح السرعة المفرطة التي تسير بها هاته الظواهر الإجرامية الماسة بالإنترنيت والمواقع الإليكترونية ووسائطها التي عرفت شيوعا وانتشارا في كافة أرجاء المعمور، وهو ما جعل مشرعنا بعد وضعه منظومة قانونية تعاقب على المس بذلك، يصدر قانونا أو منظومة إن صح التعبير، لتوفير بيئة آمنة للبيانات والعمليات الرقمية وإرجاع الثقة في المعاملات الإليكتروني، وهو ما أهل استراتيجية الأمن السيبراني الأهمية القصوى في استراتيجية الأمن القومي والإقتصادي للمغرب.

ولهذا جاء 08-09 المتعلق بحماية المعطيات ذات الطابع الشخصي والقانون 05-20 الخاص "**بالأمن السيبراني**" والقانون رقم 43-20 المتعلق "**بخدمات الثقة بشأن المعاملات الإليكترونية**" لتعزيز قدرة المملكة على مواجهة الثورة الرقمية العامة على مستوى تحديات الأمن السيبراني لإعطاء الفرصة للدولة للتدبير الأمثل للمعلومة على المستوى الوطني على صعيد جميع القطاعات، والرفع من نجاعتها في مجال أمن نظم المعلومات في الإدارات والهيآت العامة لتأطير خدمات الثقة اللازمة لحسن سير المعاملات الإليكترونية، وباعتبارنا جمعية مهنية قضائية فنؤكد أن المغرب وضع استراتيجية على صعيد جهاز العدالة لتنزيل المحكمة الرقمية ورقمنة الخدمات بالمحاكم، وتكوين القضاة وأطر كتابة الضبط في مجال الخدمات الإليكترونية لخوض غمار هذا الرهان، كما تمت مناداة جناح العدالة الثاني وهو السادة المحامون وكافة الفاعلين في مجال المهن القانونية والقضائية وكل من له صلة بمرفق العدالة لمواكبة هذا السعي.

إلا أننا نعترف بالتأخر الذي حصل في هذا الميدان، إلى أن طل علينا شبح وباء كورونا-كوفيد 19- واضطررنا لإعلان حالة الطوارئ، فشلت الخدمات والإدارات، وتم تقييد حركة النقل على المستوى

الوطني والدولي، وهو ما سبب أزمات وعقبات غير متوقعة، خيمت على المجالات والإقتصادية والسياسية أدت إلى تعليق كل مناحي الحياة الطبيعية للأفراد والجماعات، ومنها جهاز القضاء، حيث أصبح متعذرا على المرتفقين اللجوء إلى المحاكم لتقديم الشكايات أو الدعاوى أو اقتضاء الحقوق، وهو ما ضرب حق التقاضي في مقتل وكان لزاما التفكير لإيجاد سبل ومخارج لهذا الوضع المتأزم بشكل عاجل، يمكن من تفادي الأسوأ وتعليق المحاكمات وعقد الجلسات وتنظيم عجلة الحياة القضائية، حيث تم تشجيع التعاطي مع وضع المقالات عبر البوابات الإليكترونية التي أحدثتها وزارة العدل وغيرها من التطبيقات لتتبع الملفات وكافة الإجراءات عن طريق موقع"**محاكم**" مثلا الذي أحدث لهذا الغرض ولقي نجاحا واستحسانا منقطع النظير، وكذا تسهيل الحصول على بعض الوثائق إليكترونيا، وظهرت إلى العلن المحاكمات عن بعد باستعمال تقنية الفيديو، الأمر الذي أدى إلى حدوث تغييرات عميقة في نظام المحاكمات الجنحية خصوصا.

وهذا الأمر وإن كان قد ساهم في تخفيف العبء المادي على مكونات الجهاز القضائي وعلى مرتفقي العدالة، وساهم في تطوير خدماته وسرعة إجراءاته، وتقليص آجال البت للوصول إلى المبتغى الذي سنته الدولة منذ عشرات السنين وهو برنامج "**المحكمة الرقمية**"، فإنه لم يسلم من خلق نقاش حاد حول محافظته على شروط المحاكمة العادلة وعلى توفير سبلها وأسسها، وضمان السرية المحيطة بها، وهو ما أسال مدادا كثيرا عن توفر الضمانات والشروط من عدمها، وأيا كان الأمر فقد ساهم هذا الإنجاز في تحريك عجلة الجهاز القضائي وعدم بقائها جامدة مع ما يعنيه ذلك من تبعات وآثار سلبية، قد تشكل ضربا للأمن السيبراني خصوصا مع ضرورة الحفاظ على السرية التي تشكل عماد ما يناقش أمام القضاء من وثائق ودفوع ومحاكمات، التي قد يشكل خرق سريتها وانتهاك حرمتها وضعا خطيرا قد يعصف بحياة الأفراد والجماعات، ونحن كقضاة نقر بأن القاضي الجنائي يصطدم بمطبات واقعية وقانونية أثناء مناقشة وسائل إثبات الجرائم الإليكترونية كتجسيد للأمن السيبراني في ظل فراغ تشريعي متكامل موضوعا وإجراءات، وهو ما يلقي على عاتق القضاة مهاما كبيرة، قد تتجاوز القدرات المتاحة لهم أو التي يستوعبها النص القانوني والتي تلقوا تكوينا بشأنها، لاسيما وأن ارتباطها له علاقة كبرى بالمجال التقني دون القانوني، والتطور العلمي المتسارع والجارف قد يزيد من استفحال مهمة القاضي في المجال

السيبراني لكون الإثبات الرقمي من أعقد الأمور في الميدان القضائي، لا سيما في غياب الدعامات الورقية والإليكترونية.

وقد حاولنا في نادي قضاة المغرب كجمعية مهنية الإدلاء بدلونا في هذا الموضوع الهام الذي نبتغي من ورائه إبراز العراقيل والعقبات في المجال السيبراني وتحدياته الأمنية وتسليط الضوء على التوجهات الإستراتيجية في قوانيننا الوطنية وإبراز إيجابياتها وسلبياتها، واقتراح بعض الأفكار والرؤى في المجال علها تشكل توصيات تنير درب الباحثين والمهتمين بالمجال لربطها بالتنمية الاقتصادية والإجتماعية لبلداننا العربية لتشجيع مشرعيها على التعاطي مع الظاهرة بالأهمية اللازمة لخلق أمن سيبراني رائد، وقد تنوعت المواضيع التي شارك بها أعضاء جمعيتنا المهنية بين "**دور الأمن السيبراني في حماية الثقة في المعاملات الإليكترونية على ضوء القانون 20-43**" سيقدمه نائب رئيس المكتب الجهوي للنادي بمراكش الأستاذ عبد العزيز لكنيفري، و"**دور الأمن السيبراني في حماية المواقع والوسائط الإليكترونية**" سيتطرق له عضو المكتب الجهوى لنادي قضاة المغرب بمراكش الأستاذ عبد اللطيف آيت إبراهيم.

فيما سيتناول عضو نادي قضاة المغرب الأستاذ محمد أمين سيف موضوع "**حماية المستهلك الإليكتروني على ضوء الأمن السيبراني بالمغرب**" بالدراسة والتحليل، وسيقوم زملاؤنا في جمعية الودادية الحسنية للقضاة بمراكش كذلك بإماطة اللثام عن مجموعة من المواضيع التي لها ارتباط بالجهاز القضائي والأمن السيبراني.

أصحاب المعالي والسعادة، وفق الله مؤتمركم لما فيه الخير والصلاح، وكلل أعمالكم ومجهوداتكم بالتوفيق والنجاح، "**وقل اعملوا فسيرى الله عملكم ورسوله والمؤمنون**" صدق الله العظيم والسلام عليكم ورحمة الله تعالى وبركاته.

كلمة الأستاذ بدر صبور

مدير المركز الدولي للخبرة الاستشاري

بسم الله الرحمن الرحيم

الحمد لله رب العالمين والصلاة والسلام على اشرف المرسلين سيدنا محمد الصادق الأمين وبعد.

- السيد رئيس المركز الدولي للخبرة الاستشاري.
- السيد نقيب هيئة المحامين بمراكش.
- السيد عميد كلية العلوم القانونية والاقتصادية والاجتماعية جامعة القاضي عياض مراكش
- السيد رئيس المكتب الجهوي للودادية الحسنية للقضاة بدائرة محكمة الاستئناف بمراكش.
- السيد منسق ماستر العلوم الجنائية والأمنية،بكلية العلوم القانونية ولاقتصادية والاجتماعية جامعة القاضي عياض مراكش.
- السيد مدير مختبر البحث قانون الأعمال، كلية العلوم القانونية والسياسية جامعة الحسن الأول بسطات.
- السيد منسق ماستر المعاملات الالكترونية، بكلية العلوم القانونية والسياسية جامعة الحسن الأول بسطات.
- السيد محمد رافع رئيس المكتب الجهوي لنادي قضاة المغرب بمراكش.
- السيد مدير مجلة القانون والإعمال الدولية.
- السيد ممثل للجنة المنظمة.
- السيدات والسادة المشاركين في المؤتمر .
- السيدات والسادة الحضور كل باسمه وصفته .

بداية أحييكم باسم المركز الدولي للخبرة الاستشاري وأنقل لكم تحيات جمع أعضائه.

يأتي انعقاد المؤتمر العلمي الدولي حول الأمن السيبراني في تشريعات الدول العربية بعد النجاح الذي حققه المؤتمر الدولي العلمي الثالث حول الإعلام عبر الوسائط الالكترونية الذي انعقد عن بعد

بمشاركة عربية ودولية واسعة بتاريخ 17و18 يوليوز 2020 وكذلك المؤتمرين الأول الذي انعقد بمدينة اكادير بتاريخ 13 يونيو 2015 والثاني الذي انعقد بمدينة العيون بتاريخ 27 ابريل 2018 .

وها هو ينعقد مؤتمر اليوم بمدينة مراكش بشراكة مع كل من هيئة المحامين بمراكش، والمكتب الجهوي للودادية الحسنية للقضاة بدائرة محكمة الاستئناف بمراكش، والمكتب الجهوي لنادي قضاة المغرب بمراكش، وماستر العلوم الجنائية والأمنية، بكلية العلوم القانونية ولاقتصادية والاجتماعية جامعة القاضي عياض مراكش، ومختبر البحث قانون الأعمال، كلية العلوم القانونية والسياسية جامعة الحسن الأول بسطات، وماستر المعاملات الالكترونية، بكلية العلوم القانونية والسياسية جامعة الحسن الأول بسطات، ومجلة القانون والإعمال الدولية.

السيدات والسادة:

إن المركز الدولي للخبرة الاستشاري أخذ على عاتقه منذ بداية تأسيسه إلى إقامة العديد من المؤتمرات العلمية، لإيمانه أن مثل هذه المؤتمرات المتخصصة تعمل على تعميق الفائدة ومواكبة التطورات والمستجدات في هذه المجالات الجديدة.

الحضور الكريم:

إنه لمن دواعي السرور أن التقي اليوم بنخبة من رجال الفكر والقانون في الوطن العربي والمشاركة في هذا المؤتمر والذي يعتبر موضوعه حقيقة واقعـية في معظم نواحي الحياة في المجتمعات المعاصرة.كما يطيب لي أن أعبر عن تقديري الخالص لجميع المشاركين في هذا المؤتمر تعبيرا منكم عن روح ثابتة تسعى إلى تقرير الرقي بالبحث العلمي والنهوض بمجريات الحياة عن طريق مواكبة ركب التقدم والحضارة الإنسانية.

وكلنا أمل أن تثمر البحوث والدراسات المقدمة في هذا المؤتمر على تحقيق الأهداف التي سطرها المؤتمر والتي سعينا من أجلها جميعا والخروج بتوصيات ناجعة تحقق الأهداف المنشودة منه.

والسلام عليكم ورحمة الله وبركاته

كلمة الدكتور مصطفى الفوركي

مدير مجلة القانون والأعمال الدولية

بسم الله الرحمن الرحيم

السلام عليكم ورحمة الله

أولا اود ان ارحب بكافة الأساتذة المشاركين في هذا الحفل العلمي المتميز سواء الحاضرين فعليا او عن بعد و اثني على اللجنة المنظمة التي استطاعت كسب الرهان و تنظيم مثل هكذا مؤتمر بهذه المواصفات العالمية في وقت وجيز فلكم مني كل عبارة التقدير و الثناء

فباسمي و باسم مجلة القانون و الأعمال الدولية نرحب بكافة المتدخلين الكرام و كذلك بكل الحاضرين في فعاليات هذا المؤتمر المهم والذي يتناول موضوع الامن السيبيرياني في تشريعات الدول العربية

حقيقة هذا الموضوع يعتبر من الأهمية بمكان نظرا للتطورات الحاصلة في المجتمع سواء الدولي او الداخلي و الاعتماد بشكل كبير على المعطيات الرقمية و المعاملات الالكترونية في تلبية الحاجات اليومية سواء العادية منها او المعاملات المرفقية مع الإدارة و امام هذا الامر كان لزاما على المشرع ان يواكب هذه التحولات عن طريق سن تشريعات تواكب الجانب العملي والتطبيقي و التطور التكنولوجي و الالكتروني

لن ادخل في غمار الموضوع

وقبل ان اعيد الكلمة الى السيد الرئيس لا بأس ان نعطي نبذة تعريفية عن مجلة القانون والأعمال الدولية ودورها في نشر الثقافة و الوعي القانوني على خصوصا على المستوى الالكتروني

فالمجلة تأسست في سنة 2011 من رحم مختبر البحث قانون الأعمال بجامعة الحسن الأول بسطات لتبصم على مشوار متميز منذ تأسيسها تكلل بإصدار 35 اصدار بمشاركة أساتذة و ممارسين من مختلف الجنسيات، ينشر عبر الموقع الرسمي للمجلة و يوزع على مختلف دول العالم و 8 مؤلفات جماعية خاصة

كما انبثقت عن المجلة سلسلة فرعية تعنى بنشر الأبحاث من اطاريح الدكتوراه و رسائل الماستر في شكل كتب الكترونية وقد وصلنا الى العدد رقم 32 من سلسلة الدراسات و الأبحاث الجامعية و الاكاديمية

بالإضافة الى ان موقع المجلة أصبح موسوعة قانونية بامتياز باحتوائه على 100 الف محتوى قانوني موزع ما بين المقالات و الأبحاث و التقارير و نشر الاحكام و القرارات القضائية

ومن جهة أخرى المجلة شاركت في تنظيم العديد من اللقاءات الوطنية والمؤتمرات الدولية

كما ان المجلة معتمدة دوليا من مختلف جامعات الدول العربية وحائزة على تصنيف جد متقدم في منظمة ا س ا اندكنسنغ للارشفة الدولية و كذا تصنيف متقدم في مؤشر التصنيف الخاص باتحاد الجامعات العربية كما ان المجلة معتمدة من طرف المعهد المغربي للاعلام العلمي و التقني IMIST

هذه بعجالة اهم المحطات التي مرت بها المجلة من خلال مشوارها الى غاية الان

وأتمنى من العلي القدير ان يكون هذا المؤتمر محفلا علميا ناجحا زاخرا بالمداخلات والأبحاث القيمة والتي ستغني النقاش

في الأخير اشكر الدكتور ضياء نعمان على تميزه الدائم وعلى تنظيمه المحكم لفعاليات هذا المؤتمر وعلى مجهوده الكبير

ولكي لا اطيل احيل الكلمة مباشرة الى السيد الرئيس

كلمة الأستاذ أيوب بودو

محام بهيئة المحامين بمراكش ممثلا للجنة المنظمة

بسم الله الرحمن الرحيم

- السيد رئيس المركز الدولي للخبرة الاستشاري.

- السيد نقيب هيئة المحامين بمراكش.

- السيد عميد كلية العلوم القانونية والاقتصادية والاجتماعية جامعة القاضي عياض مراكش

- السيد رئيس المكتب الجهوي للودادية الحسنية للقضاة بدائرة محكمة الاستئناف بمراكش.

-السيد رئيس المكتب الجهوي لنادي قضاة المغرب بمراكش

- السيد منسق ماستر العلوم الجنائية والأمنية، بكلية العلوم القانونية ولاقتصادية والاجتماعية جامعة القاضي عياض مراكش.

- السيد مدير مختبر البحث قانون الأعمال، كلية العلوم القانونية والسياسية جامعة الحسن الأول بسطات.

- السيد منسق ماستر المعاملات الالكترونية، بكلية العلوم القانونية والسياسية جامعة الحسن الأول بسطات.

- السيد مدير مجلة القانون والإعمال الدولية.

-السيدات والسادة الحضور.

لي عظيم الشرف أن انوب عن اللجنة المنظمة بإلقاء كلمتها في هذا الحفل العلمي، وهي مناسبة أن أتقدم بالشكر الجزيل أصالة عن نفسي ونيابة عن جميع أعضاء اللجنة المنظمة لكل من ساهم في الإعداد لهذا المؤتمر وهم المركز الدولي للخبرة الاستشاري،وهئية المحامين بمراكش، والمكتب الجهوي للودادية الحسنية للقضاة بدائرة محكمة الاستئناف بمراكش، والمكتب الجهوي لنادي قضاة المغرب بمراكش، وماستر العلوم الجنائية والأمنية،بكلية العلوم القانونية ولاقتصادية والاجتماعية جامعة القاضي عياض مراكش، ومختبر البحث قانون الأعمال، كلية العلوم القانونية والسياسية جامعة الحسن الأول

بسطات، وماستر المعاملات الالكترونية، بكلية العلوم القانونية والسياسية جامعة الحسن الأول بسطات، ومجلة القانون والإعمال الدولية.

كما أرحب وباسم اللجنة المنظمة بجميع السيدات والسادة المشاركين في هذا المؤتمر العلمي الدولي، والذين عبروا بصدق عن هم الباحث الأكاديمي وهدفه النبيل المتجسد بخدمة العلم والمعرفة.

الحضور الكريم:

لقد تم اختيار الأمن السيبراني في تشريعات الدول العربية، عنوانا لهذا المؤتمر وهو الموضوع المتداول على الألسن والمثبوت في صفحات الجرائد والمواقع الإخبارية الالكترونية، وفي الدراسات والأبحاث، وكذا وثائق الإدارات وأحكام وقرارات المحاكم.

وقد استعمل استعمالات ذات مرجعيات مختلفة، استعمله الأمني والسياسي والإعلامي والفقيه والباحث الأكاديمي في العلوم القانونية.

السيدات والسادة الحضور:

معلوم أن فضاء البحث العلمي هو فضاء التفكير في الإشكالات العلمية ومقاربتها وبلورة مشاريع بحثية وتكوينية، وهذا ما ننتظره من هذا المؤتمر ومن المشاركين فيها والأمل معقود على مخرجاتها.

الحضور الكريم:

إن مؤتمر الأمن السيبراني في تشريعات الدول العربية، ركز على أهداف معينة بذاتها، وتتمثل هذه الأهداف في:

- تعزيز دور البحث العلمي في مجال الأمن السيبراني.
- تسليط الضوء على التوجهات الإستراتيجية في تشريعات الدول العربية في مجال الأمن السيبراني.
- إبراز ايجابيات وسلبيات تشريعات الأمن السيبراني في الدول العربية.
- معرفة الرؤية النظرية المطروحة للأمن السيبراني.
- معرفة الدور الذي يقوم به الأمن السيبراني في التنمية الاقتصادية والاجتماعية.

ولتحقيق هذه الأهداف انعقد هذا المؤتمر بمشاركة ذات بعد دولي لعدة دول هي: المملكة المغربية، اليمن، الجزائر، قطر، موريتانيا، ليبيا، مصر، الأردن، السودان، سلطنة عمان، الإمارات العربية المتحدة، العراق، مملكة البحرين، وبريطانيا.

فمرحبا بكل ضيوفنا الكرام ونسأل الله التوفيق والسداد في مناظراتكم العلمية، كما نتوجه بالشكر لكل من أسهم من قريب أو بعيد في إنجاح أشغال هذا المؤتمر.

والسلام عليكم ورحمة الله وبركاته.

الجلسة العلمية الأولى

رئيس الجلسة

محمد الحميدي

نقيب هيئة المحامين بمراكش

الأمن السيبراني في حماية أنظمة العدالة

الدكتور ثاني بن علي آل ثاني
مؤسس مكتب ثاني بن علي للمحاماة والاستشارات
القانونية والتحكيم (قطر)

المقدمة

أصبح الأمن السيبراني حجر الزاوية في أي سياسة أمنية وطنية ولعل قطر من أهم الدول التي تأذت من تبعات واعتداءات وضحت أهدافها وصورها للعيان مما ألهب أيدي ونفوس صناع السياسات والقرارات على مستوى العالم على أن يصنفوا مسائل الدفاع والأمن السيبراني، وحماية وأمن المعلومات كأولوية عليا في سياساتهم الدفاعية الوطنية، مما حدا بالكثير من دول العالم بأن يخصصوا أقساماً وسيناريوهات خاصة لخوض هذه الحروب السيبرانية ضمن فرق الأمن الوطني تضاف إلى الفرق الأمنية التقليدية لمحاربة الجرائم الإلكترونية.

ولعلي أرى أن الأمن المعلوماتي ليس فقط أمن وطني ولكن هذا العمل من أهم مقتضيات الاقتصاد الوطني فالأسرار الاقتصادية تفوق الأسرار العسكرية والحربية في هذا الزمان.

كما أن أمن المجتمع وخصوصيات الأفراد والأسر والعائلات أهم بكثير من الأسرار الاقتصادية لأن الفرد والأسرة هما عماد الدولة وقوة وتماسك المجتمع، لذا يجب علينا أن نبدأ بالفرد والأسرة أولاً من خلال حملات توعية تكون سهلة وبسيطة لتحقق أهدافها بتثقيف الفرد والأسرة والمجتمع بهذه الجريمة وأساليبها والآثار الناجمة عنها إذن فهي ليست مسؤولية الدولة أو الحكومات فقط ولكنها مسؤولية مجتمعية.

والله أسأل أن يوفقنا جميعاً،

أهم التشريعات في قطر

استهلت قطر عامها الحالي بالقرار الأميري رقم (1) وهذه دلالة خاصة على أن يكون القرار الأول في عام 2021م بإنشاء الوكالة الوطنية للأمن السيبراني وذلك بعد الاطلاع على:

1- القرار الأميري رقم (16) لسنة 2014م بتعيين اختصاصات الوزارات.
2- القرار الأميري رقم (48) لسنة 2014م بالهيكل التنظيمي لوزارة الداخلية، المعدل بالقرار رقم (8) لسنة 2015م.
3- القرار الأميري رقم (19) لسنة 2016م بإنشاء اللجنة الوطنية لأمن المعلومات، المعدل بالقرار الأمير رقم (18) لسنة 2019م.
4- قرار مجلس الوزراء رقم (26) لسنة 2018م بتعديل تنظيم بعض الوحدات الإدارية التي تتألف منها وزارة المواصلات والاتصالات وتعيين اختصاصاتها.
5- قرار وزير الداخلية رقم (30) لسنة 2018م بتعديل مسمى واختصاصات مركز أمن المعلومات.
6- قرار وزير الداخلية رقم (57) لسنة 2018م بالهيكل التنظيمي لمركز الأمن الإلكتروني.
7- قرار رئيس اللجنة الأمنية باللجنة العليا للمشاريع والإرث رقم (4) لسنة 2020م بإنشاء لجنة عمليات أمن وسلامة بطولة كأس العالم فيفا قطر 2022 وتعيين اختصاصاتها.

وهذه الوكالة تهدف إلى المحافظة على الأمن السيبراني وتنظيمه، وتعزيز المصالح الحيوية للدولة وحمايتها في مواجهة تهديدات الفضاء السيبراني، ويكون لها في سبيل تحقيق ذلك ممارسة كافة الاختصاصات والصلاحيات وذلك خلال ما يلي:

1- إعداد الاستراتيجية الوطنية للأمن السيبراني وتحديثها بالتنسيق مع الجهات المعنية والاشراف على تنفيذها بعد اعتمادها من مجلس الوزراء.
2- وضع وتحديث السياسات وآليات الحوكمة والمعايير والضوابط والارشادات اللازمة لتعزيز الأمن السيبراني بالتنسيق مع الجهات المعنية وتعميمها على الجهات ذات العلاقة ومتابعة الالتزام بها.
3- وضع وتحديث أطر إدارة المخاطر السيبرانية ومتابعة الالتزام بها.
4- تقييم الوضع الأمني السيبراني في الدولة، بالتنسيق مع الجهات المعنية لرصد المخاطر بصفة استباقية.
5- إعداد التقارير عن الحالة الأمنية السيبرانية محلياً وإقليمياً ودولياً.
6- تحديد وتصنيف مؤسسات القطاعات الحيوية في الدولة.

7- إعداد وتنفيذ الخطة الوطنية للاستجابة والتعافي من الحوادث والهجمات السيبرانية بالتنسيق مع الجهات المعنية.

8- الاشراف على خطط الطوارئ وضمان استمرارية الأعمال المتعلقة بالأمن السيبراني لمؤسسات القطاعات الحيوية.

9- وضع آليات لتبادل ومشاركة ونشر ورصد واستطلاع وتحليل المعلومات المتعلقة بالأمن السيبراني مع الجهات المحلية والدولية.

10- وضع المعايير والآليات اللازمة لفحص واعتماد الأجهزة والأنظمة والتطبيقات المشغلة للبنية التحتية الحيوية في الدولي بالتنسيق مع الجهات المعنية.

11- إجراء الاختبارات الفنية للأنظمة والبرامج والشبكات في مؤسسات القطاعات الحيوية.

12- اعتماد أطر ومعايير تقييم الكوادر البشرية العاجلة بمجال الأمن السيبراني في مؤسسات القطاعات الحيوية.

13- تقييم وتطوير قدرات الأمن السيبراني لمؤسسات القطاعات الحيوية ووضع خطط لرفع المستويات ومتابعة تنفيذها.

14- وضع معايير وضوابط الترخيص لمقدمي خدمات الأمن السيبراني وإصدار شهادات الاعتماد.

15- رفع مستوى الوعي بالأمن السيبراني ودعم وتطوير القدرات الوطنية في هذا المجال من خلال البرامج والمبادرات وتنظيم الفعاليات المتعلقة بالأمن السيبراني في الدولة.

16- اعتماد مشاريع ومبادرات الأمن السيبراني في مؤسسات القطاعات الحيوية.

17- تنفيذ تمارين الجاهزية والمناورات السيبرانية على مستوى الدولة.

18- إبرام العقود ومذكرات التفاهم والشراكات مع الجهات المحلية والدولية المعنية بالأمن السيبراني.

19- متابعة تنفيذ التزامات الدولة المعنية بالأمن السيبراني.

20- تشجيع وتوجيه البحث العلمي والابتكار في مجال الأمن السيبراني، والعمل على توطين صناعة محلية له.

21- تنفيذ القوانين واللوائح والقرارات المتعلقة بحماية خصوصية البيانات الشخصية.

22- اقتراح الأدوات التشريعية ذات الصلة بالأمن السيبراني.

وتلتزم جميع الجهات في الدولة بالتعاون مع هذه الوكالة في أداء مهامها، وموافاتها بما تطلبه من معلومات وبيانات لازمة لأداء عملها، كما تلتزم تلك الجهات بتنفيذ السياسات والقرارات والتعاميم التي تصدرها الوكالة في مجال اختصاصها.

وتتحمل تلك الجهات مسؤولياتها في حماية أنظمتها المعلوماتية ومواقعها الإلكترونية وشبكاتها المعلوماتية والبيانات والمعلومات الإلكترونية الخاصة بها واتخاذ التدابير الأمنية الوقائية اللازمة، بما لا يتعارض مع اختصاصات الوكالة.

أهم التشريعات للحماية السيبرانية الإسكوا

لقد دخلت الدول العربية إلى عالم تشريع الفضاء السيبراني متأخرة بعض الشيء عن الدول الغربية كما هو حال دول العالم الجنوبي عموماً خاصة وأن بناء مجتمع معلوماتي قد استعدت له الدول المتقدمة منذ عقد الثمانينات ويضاف إلى ذلك أن الاعتماد على شبكات وأنظمة الحاسوب في المعاملات والتجارة وفي مجال القطاع العام بصفة خاصة في الدول العربية لم تأخذ بنصيب وافر مما هو عليه دول الاتحاد الأوروبي وجنوب شرق آسيا وأمريكا الشمالية من التكنولوجيا.

وعلى الرغم من ذلك فإن استعمال أجهزة وأنظمة الحاسوب أخذت تتزايد بشكل ملحوظ يوماً بعد يوم في الدول العربية وبالتالي ازدادت الحاجة إلى تنظيم قانوني لاستعمال هذه الأنظمة لا سيما بعد أن واكب القطاع الخاص والاستثماري والأفراد منفردين التطور الحادث وبدأ استعمال شبكة الانترنت الفعلي لأجل القيام بعمليات مصرفية أو معاملات أو تعاقدات وازدادت الحاجة إلى هذه الشبكة بصورة أكثر بعد إعلان كوفيد 19 جائحة عالمية وبدء العمل بصيغة التباعد الاجتماعي وتوقف حركة السفر واللقاءات ولكن للحقيقة كانت هناك بعض الدول بعيدة كل البعد عن هذه الشبكة العنكبوتية وآثاره التكنولوجية إلى وقت قريب.

وأمام هذا الغياب في التشريع السيبراني في بعض الدول العربية قامت بعض الدول في بداية الأمر باقتباس قوانين بعض الدول الأوروبية ومحاولة ملاءمتها مع الواقع القائم في الدول العربية المعنية لإقرار هذه القوانين.

وقد تم أيضاً الاسترشاد بالمعاهدات والاتفاقيات الدولية والنماذج القانونية لمنظمات دولية مثل الأونسترال UNCTRAL في ورشة التشريع العربية وتختلف المقارنات التشريعية في الدول العربية من ناحية تقنين مواضيع الفضاء السيبراني والذي يمكن إيجازه فيما يلي:

أ) وضع قانون خاص لكل موضوع من مواضيع الفضاء السيبراني.

ب) تعديل القوانين القائمة والسارية المفعول وإضافة مواد أو فصول عليها تتعلق بالفضاء السيبراني، والتي تتبين لاحقاً أن هذه الطريقة لا تلبي الحاجة التشريعية حيث اقتصر الأمر على بعض المواضيع مثل قانون حماية حق المؤلف والاثبات الإلكتروني اللذين تم تناولهما ضمن إطار قوانين الإجراءات وأصول المحاكمات المدنية.

ت) وضع قانون موحد يشمل مختلف مواضيع الفضاء السيبراني ويكون نصاً واحداً مقسماً إلى أبواب يتعلق كل منها بموضوع من مواضيع الفضاء السيبراني.

ث) وتعتبر التشريعات السيبرانية مكوناً أساسياً من مكونات البيئة التنظيمية والقانونية اللازمة لتطوير مجتمع المعلومات.

كما تشكل عنصراً هاماً لتوفير الثقة بالخدمات الإلكترونية وتأمين الحماية لمستخدمي الفضاء السيبراني، ومن هذا المنطلق وبهدف تعزيز مجتمع المعرفة في المنطقة العربية والمساهمة في تحفيز التكامل الإقليمي، بدأ اهتمام اللجنة الاقتصادية والاجتماعية لغرب آسيا (الإسكوا) بتطوير التشريعات السيبرانية CyberLaws كونها تشكل عنصراً أساسياً من عناصر البيئة التمكينية لمجتمع المعلومات ولبناء الاقتصاد المبني على المعرفة.

ولقد قامت منظمة الإسكوا في عام 2007م بإعداد عدة دراسات حول وضع التشريعات السيبرانية في الدول العربية.

ومنذ هذا التاريخ قامت أيضاً بتنظيم عدة اجتماعات خبراء لمناقشة هذه الدراسات وتحديد احتياجات المنطقة من أجل تحسين وضع التشريعات السيبرانية.

وفي سبيل تحسين التجارة الإلكترونية البينية ومواجهة الجرائم السيبرانية وبناء اقتصاد إقليمي مبني على المعرفة باشرت الإسكوا عام 2009م بإعداد وتنفيذ مشروع "تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية" للاستجابة لاحتياجات المنطقة العربية في مجال التشريعات السيبرانية.

وسوف نعرض أهم الدول المنضمة إلى الإسكوا والتي عملت على إصدار تشريعات خاصة بتنظيم الاتصالات وهي كالآتي:

1- المملكة الأردنية الهاشمية – قانون الاتصالات رقم (13) لسنة 1995م.

2- الإمارات العربية المتحدة – القانون الاتحادي رقم (3) لسنة 2003م وتعديلاته بشأن تنظيم الاتصالات.

3- مملكة البحرين – مرسوم بقانون رقم (48) لسنة 2002م بإصدار قانون الاتصالات.

4- سلطنة عمان – قانون تنظيم الاتصالات بموجب المرسوم السلطاني رقم (30) لسنة 2002م الخاص بتنظيم الاتصالات.

5- سوريا – قانون رقم (18) لسنة 2010م الخاص بالاتصالات.

6- السودان – قانو الاتصالات لسنة 2001مز

7- العراق – قانون الاتصالات اللاسلكية رقم (159) لسنة 1980م.

8- فلسطين – قانون الاتصالات الفلسطيني لسنة 2005م.

9- قطر – مرسوم بقانون رقم (34) لسنة 2006م بإصدار قانون الاتصالات.

10- الكويت- مشروع قانون الاتصالات الكويتي عام 2010م.

11- لبنان – قانون تنظيم قطاع خدمات الاتصالات على الأراضي اللبنانية رقم (431) صادر في 2002/7/22م.

12- مصر- قانون الاتصالات المصري رقم (10) لسنة 2003م.

13- السعودية – مرسوم ملكي رقم (م/12) الصادر في 1422/3/12ه الخاص بنظام الاتصالات- لائحة النظر في مخالفات نظام الاتصالات.

14- اليمن – مشروع قانون الاتصالات وتقنية المعلومات.

أهم ما اشتملت عليه التشريعات الوطنية الخاصة لحماية أمن المعلومات / الأمن السيبراني

لقد كرست جميع الدساتير العربية مبدأ سرية المراسلات والاتصالات السلكية وحدد بعضها مبدأ عدم جواز مراقبتها أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها إلا في الحالات التي يبينها القانون وبأمر قضائي مثل الدستور اليمني، حيث نصت المادة (53) منه على "حرية وسرية المواصلات البريدية والهاتفية والبرقية وكافة وسائل الاتصالات مكفولة ولا يجوز مراقبتها أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها إلا في الحالات التي يبينها القانون وبأمر قضائي".

كما أكدت بعض قوانين الاتصالات الوطنية الخاصة على سرية وخصوصية الاتصالات مثال قانون البحرين رقم (18) لسنة 2002م الخاص بتنظيم الاتصالات حيث نصت المادة (3) منه على "أن من مهام وصلاحية هيئة تنظيم الاتصالات حماية البيانات الخاصة وخصوصية الخدمات".

وقد حدد القانون السعودي لتنظيم الاتصالات الصادر عام 2001م في المادة رقم (9) منه على " أن سرية المكالمات الهاتفية والمعلومات التي يتم إرسالها أو استقبالها عبر شبكات الاتصالات العامة مصونة، ولا يجوز الاطلاع عليها أو الاستماع إليها أو تسجيلها إلا في الحالات التي تبينها الأنظمة".

كما حدد قانون الاتصالات المصري رقم (10) لسنة 2003م البند (6) من المادة رقم (5) منه على " أن من مهام الجهاز القومي لتنظيم الاتصالات ...." 6- وضع القواعد التي تضمن حماية المستخدمين بما يكفل سرية الاتصالات وتوفير أحدث خدماتها".

أما القانون السوري الصادر عام 2010م منذ نص في المادة الثالثة منه على "أن من مهام الهيئة الناظمة لقطاع الاتصالات (الفقرة (و) البند (4)) "الحفاظ على سرية المعلومات الناجمة عن تقديم الخدمات وخصوصيتها" كما أفرد هذا القانون باباً خاصاً لحماية البيانات والخصوصية والأمن القومي حيث تكون للاتصالات بين المستخدمين صفة السرية (الخصوصية) كما يتخذ كل مرخص له جميع الإجراءات الكفيلة بضمان سرية وخصوصية بيانات المشتركين لديه.

كما تحدد اللائحة التنفيذية لهذا القانون شروط حماية بيانات الحركة وخصوصية بيانات موقع المشترك".

وشملت قوانين أخرى خاصة بتنظيم الاتصالات على فرض عقوبات عند مخالفة هذه الأحكام وخرق أمن شبكة الاتصالات، مثال:

- الإمارات العربية المتحدة حيث جاء في المادة (72) من قانون تنظيم قطاع الاتصال لسنة 2003م "يعاقب بالحبس مدة لا تزيد عن كل من استغل أجهزة الاتصالات في الإساءة أو الازعاج أو إيذاء مشاعر الآخرين أو لغرض آخر غير مشروع، كل من نسخ أو أفشى أو وزع بدون وجه حق فحوى أي اتصال أو رسالة هاتفية أو أي من خدمات الاتصالات".

- أما القانون المصري الخاص بتنظيم الاتصالات فقد نص في المادة (73) منه على أن "يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تزيد عن كل من قام أثناء تأدية وظيفته في مجال الاتصالات أو بسببها بأحد الأفعال التالية:

1- إذاعة أو نشر أو تسجيل لمضمون رسالة اتصالات أو لجزء منها.
2- إخفاء أو تغيير أو إعاقة أو تحوير أية رسالة اتصالات.
3- إفشاء أية معلومات خاصة بمستخدمي شبكات الاتصال أو عما يجرونه أو ما يتلقونه من اتصالات وذلك دون وجه حق".

واكتفت بعض الدول العربية بالإحالة إلى قوانين عامة عند خرق مبدأ سرية الاتصالات، مثال قانون العقوبات اللبناني حيث جاء في الفصل الثاني من الباب الثامن: " في الجرائم الواقعة على الحرية والشرف" وقد تضمن هذا الفصل نبذة خاصة عنوانها "في إفشاء الأسرار" (المواد من 579 إلى 581)، كما وحددت القوانين الخاصة بتنظيم الاتصالات مسؤولية وواجبات مقدمي خدمات الاتصالات في المحافظة على سرية المعلومات ونذكر منها على سبيل المثال:

- قانون قطر رقم (34) لسنة 2006م الخاص بإصدار قانون الاتصالات والذي نص في المادة رقم (52) منه: (حماية معلومات العملاء) "على مقدمي الخدمة عند إدارة شبكاتهم ومرافقها والأنظمة المتصلة بها مراعاة حقوق الخصوصية للعميل، وتقع عليهم مسؤولية حفظ المعلومات والبيانات بالعميل وباتصالاته التي تكون بحيازتهم، وعليهم توفير الحماية الكافية لها، ولا يجوز لمقدم الخدمة جمع أي معلومات أو استعمالها أو الاحتفاظ بها أو إعلانها عن أي عميل إلا بموافقته أو وفقاً لما يسمح به القانون".

- وعلى مقدمي الخدمة التأكد من أن المعلومات المقدمة صحيحة وكاملة وصالحة لغرض استعمالها وللعملاء الحق في أن يطلبوا تصحيح أو حذف أي معلومات خاصة بهم.

- وليس في أحكام هذه المادة ما يمنع السلطات المختصة من الحصول على أي معلومات سرية أو اتصالات خاصة بالعملاء وفقاً للقانون".

- كما نص القانون اللبناني رقم (431) لسنة 2002م الخاص بتنظيم قطاع خدمات الاتصالات على الأراضي اللبنانية في المادة (38) (إجراءات المراقبة والتفتيش): "تعتبر المعلومات التي يطلع المراقبون والمفتشون في معرض تنفيذهم لمهامهم سرية ولا يجوز لهم البوح بها إلا أمام رؤسائهم التسلسليين أو بناءً على طلب المرجع القضائي المختص، كما تطبق أحكام السرية على كل من يطلع على هذه المعلومات بحكم عمله في الهيئة أو الوزارة".

قطر والأمن السيبراني في حماية أنظمة العدالة وحماية المجتمع

وفي ظل تطور تحديات الأمن السيبراني على مستوى العالم وخاصة في هذه الفترة الحالية وبعد عدة حوادث شهيرة على مستوى العالم تظل التطورات تتلاحق من خلال تحديات الأمن السيبراني على مستوى العالم، وتأتي حماية النظم والبنية الأساسية لتكنولوجيا المعلومات والاتصالات على رأس أولويات وزارة المواصلات والاتصالات، ولعل أهم الفوائد العظيمة التي يقدمها لنا الفضاء الإلكتروني محفوفة بعدد من التحديات التي قد تهدد البنية التحتية التي تعزز من قدرتنا على الاستخدام الآمن للإنترنت وسعياً منها لمواجهة هذه التحديات، تواصل دولة قطر بذل المزيد من الجهود الرامية إلى تعزيز الأمن السيبراني، فضلاً عن التعاون مع نظرائها حول العالم لخلق فضاء إلكتروني مفتوح وآمن ومن أجل تحقيق هذه الغاية، أنشأت الوزارة المختصة (وزارة الاتصالات وتكنولوجيا المعلومات سابقاً) ما يعرف بـ "الفريق القطري للاستجابة لطوارئ الحاسب"، المعروف باسم "كيوسرت"، في 2005م بالتعاون مع جامعة كارنيجي ميلون.

ويعمل قطاع الأمن السيبراني من خلال إدارتي "كيوسرت" و"حماية البنية التحتية للمعلومات الحيوية" مع الهيئات الحكومية وهيئات القطاعين العام والخاص ومع المواطنين القطريين لتوعيتهم بكيفية احتواء المخاطر والتهديدات التي تواجههم على شبكة الإنترنت، كما يعمل القطاع على حماية المعلومات الحيوية على شبكة الانترنت وضمان تأمينها ونظراً لأن قضايا تأمين المعلومات تتخطى الحدود الجغرافية للدولة الواحدة، فإن قطاع الأمن السيبراني عضو في المنتدى الدولي للطوارئ الحاسوبية وفرق التأمين المعروف باسم (FIRST)، حيث يدعم هذا المنتدى العلاقات الدولية التي تربط فرق التأمين بعضها ببعض والشركاء حول العالم من أجل تبادل أحدث المعلومات حول التهديدات والمخاطر التي تتعرض لها المواقع الإلكترونية الحيوية، كما أن القطاع عضو في منظمة الميريديان الدولية المعنية بأمور حماية البنية التحتية الحيوية.

الحدث الأهم عالمياً الذي أصبح نقطة فاصلة في الأمن السيبراني

شكلت جريمة قرصنة وكالة الأنباء القطرية قنا الشرارة الأولى والأكبر ونقطة الصفر في خطة التصعيد المتسارع وغير المتوقع والتي أحدثت الأزمة الأكبر في تاريخ مجلس التعاون الخليجي وهي الأزمة الخليجية والتي لا زالت تلقى بظلالها بالرغم من اتفاق العلا السعودي في مستهل عام 2021م.

ويتزامن تاريخ 24 مايو مع جريمة قرصنة وكالة ا لأنباء القطرية والتي تخطت الأعوام الثلاثة على قرصنة عدت ذريعة رئيسية لدول عربية شقيقة بهدف فرض حصاراً على قطر منذ عام 2017م، ففي الساعات الأولى من يوم 24 مايو 2017م، نشرت اقتباسات مفبركة نسبت إلى حضرة صاحب السمو أمير البلاد المفدى حفظه الله على الموقع الإلكتروني لوكالة الأنباء القطرية والحسابات التابعة لها على مواقع التواصل الاجتماعي، تبعتها حملة ممنهجة من وسائل إعلام دول الحصار، للإساءة إلى رمز الدولة وشعبها.

وقد اكتملت خيوط المؤامرة وظهرت أول تداعيات جريمة القرصنة فجر العاشر من رمضان الخامس من يونيو حين أعلنت دول الحصار الأربعة قطع علاقاتها الدبلوماسية مع قطر، كما طلبت من الدبلوماسيين القطريين المغادرة وفرضت حصاراً شاملاً على قطر يغلق كافة المجالات والمنافذ الجوية والبرية والبحرية مع قطر.

ولكن بفضل الله تجاوزت قطر كل ذلك وتحدت الحصار وأصبحت فوق الحصار وظهر الحق ووضح كرابعة النهار وعاد الحق لأصحابه ولكن تظل الجريمة السيبرانية التي أصبحت سابقة خطيرة في تاريخ العلاقات الدولية، والتي أحدثت ضجة كبيرة وأثارت استياء المجتمع الدولي مما جعل العديد من حيث من دول العالم، وعلى رأسها الولايات المتحدة الأمريكية وبريطانيا وتركيا، إعلان استعدادهم للمشاركة في التحقيقات لمساعدة قطر في التوصل لمرتكبي هذه الجريمة.

فيما أعلنت قطر أنها ستلاحق وتقاضي المسؤولين عن عملية قرصنة الموقع الرسمي لوكالة قنا، وتكاتفت الدول الشقيقة والصديقة للمشاركة في كشف المتورطين في هذه الجريمة الأخلاقية الدولية.

ولقد كانت هذه الثغرة الإلكترونية هي الدافع الأول لجميع دول العالم للانتباه والتركيز الشديد على تأمين البيانات والوثائق الحساسة وكذلك المواقع الإلكترونية وخاصة الحكومية.

وحديثاً أكدت دولة قطر على أهمية عقد مؤتمر دولي لبحث سبل تنظيم الأمن السيبراني في القانون الدولي، وهي الدعوى التـي أطلقها سمو أميـر البلاد من على منبـر الجمعية العامة للأمم المتحدة في دورتها الرابعة والسبعين حيث أكد مندوب قطر الدائم لدى الأمم المتحدة[1] والمنظمات الدولية في فيينا، في كلمة أمام الدورة الثلاثين للجنة منع الجريمة والعدالة الجنائية التابعة للأمم المتحدة إن "دولة قطر تعد من أكثـر الدول اهتماماً بتعزيز الأمن السيبراني على المستويين الوطن والدولي.

وأنشأت مطلع 2021 الوكالة الوطنية القطرية للأمن السيبراني، كما صوتت لصالح قرار أممـي لوضع اتفاقية دولية شاملة لمكافحة الجريمة السيبرانية.

هذه المعلومات، وارتباطها بالتغييرات والتطورات السريعة لتكنولوجيا المعلومات والاتصالات، وعدم التنبه باكراً لأهمية مجتمع المعلومات والاقتصاد المبنـي على المعرفة.

وبالتالي عدم تهيئة المناخ والبيئة الملائمة لنموها في العديد من بلدان المنطقة يضاف إلى ذلك بطء عملية صياغة وإقرار القوانين في معظم البلدان العربية، وذلك نتيجة لعدم الاستقرار السياسي في المنطقة كما أن تقاطع التشريعات السيبرانية مع العديد من القوانين القائمة يشكل صعوبة إضافية أمام البلدان.

لا سيما القوانين المتعلقة بتنظيم قطاع الاتصالات والتـي وضعت منذ عقود مما يجعل من تعديلها بهدف إدراج بنود خاصة بالتواصل عبـر الشبكة وبالمعاملات الإلكترونية عملية معقدة نسبياً وكذلك الأمر بالنسبة للقوانين الجزائية وقانون العقوبات، إذ أن إدخال بنود خاصة بالجريمة الإلكترونية أو إصدار قانون خاص بذلك يتطلب جهداً من أجل تحديد ماهية الجرائم الإلكترونية وكيفية إثباتها وعقوباتها، بما يتلاءم مع الإطار الفقهـي والقانوني للبلد، وقد حاولت بعض البلدان استدراك هذا الفراغ التشريعي عبـر سن قوانين في مواضع معينة، كقوانين المعاملات الإلكترونية مثلاً، وذلك باقتباس القوانين من بلدان أخرى أو بالاستعانة بالمعاهدات الدولية الملائمة.

الحاجة إلى الخبرات وتنوعها

حيث يتطلب تنوع وتشعب قوانين الفضاء السيراني، خاصة الجانب الفنـي والتشريعي منها، وجود خبـرات متنوعة في اللجان الوطنية الخاصة بصياغة هذه القوانين، كما تحتاج إلى نقاش فنـي وقانوني وفقهـي بين

[1] السفير سلطان بن سالمين المنصوري، المندوب الدائم لدولة قطر لدى الأمم المتحدة والمنظمات الدولية في فيينا 2021م.

الخبراء بحيث يصدر القانون كاملاً وخالياً من التفاصيل الدقيقة الخاصة بتكنولوجيا المعلومات والاتصالات نظماً للتغير المستمر والتطور السريع في هذه التكنولوجيا.

ونظراً لتعدد الجهات المعنية بالتشريعات السيبرانية في الدول العربية، فينبغي أن تضم لجان الصياغة ممثلين عن هذه الجهات لكي تأخذ بعين الاعتبار جميع وجهات النظر.

كما أن من المفضل في هذه اللجان وجود خبراء بالقانون والتشريع من ناحية، وبتكنولوجيا المعلومات والاتصالات، كالتشفير مثلاً بالنسبة لقانون التوقيع الإلكتروني.

بالإضافة إلى ما سبق، تتطلب صياغة القوانين والتشريعات السيبرانية الإلمام بتجارب بعض الدول وقوانينها السيبرانية، والتعرف على القوانين والتشريعات الدولية المتوفرة لأخذها بعين الاعتبار عند وضع القوانين الوطنية وذلك نظراً للطبيعة الشمولية للقضاء السيبراني ولأهمية التعاون الإقليمي والدولي في هذا المجال.

وتجدر الإشارة إلى أهمية الاستعانة بتجارب البلدان الأخرى وضرورة ملاءمتها مع الاحتياجات الوطنية والأطر الفقهية والقانونية والمجتمعية الوطنية.

وتحتاج عملية سن التشريعات السيبراني كذلك إلى منهج وطني واضح، يعتمد على إشراك كافة الجهات والهيئات أو الوزارات المعنية فانفراد جهة واحدة بعملية التشريع أو تجاوز القواعد الدستورية القائمة المنظمة لهذه العملية أو اعتبار السلطة التشريعية وحدها قادرة على تفهم وإدراك كافة الجوانب التقنية القانونية والفنية لمشروع القانون والتي يمكن أن تحدث واقعياً مما يمثل عائقاً أمام عملية سن التشريعات السيبرانية.

أهم تقسيمات مواضع التشريعات السيبرانية

اعتمدت عدة منهجيات لسد الفراغ التشريعي الخاص بالفضاء السيبراني في البلدان العربية، فقد لجأ بعضها إلى تعديل القوانين القائمة بالفعل بإضافة أبواب وبنود خاصة بالفضاء السيبراني، مثل إدراج الجريمة الإلكترونية ضمن قانون العقوبات أو القوانين العقابية الجزائية التقليدية، أو تعديل بعض مواد قانون حماية المستهلك لتغطية الجانب السيبراني.

وقد تبين أن هذه المنهجية غير كافية لأنها تنطبق على مواضيع دون أخرى ولا تلبي الحاجة السيبرانية الشاملة، وتضاءل اعتمادها نظراً لعدم كفايتها من ناحية ولتطور وتوسع تكنولوجيا المعلومات والاتصالات بشكل مستمر وتعدد تطبيقاتها من ناحية أخرى.

وتتمثل المنهجية الثانية، وهي الأكثر شيوعاً، بسن عدة قوانين يغطي كل منها محوراً أو أكثر من محاور الفضاء السيبراني كالتوقيع الإلكتروني والمعاملات الإلكترونية والجرائم الإلكتروني وقد اعتمدت بلدان عربية عديدة هذه المنهجية نظراً لسهولتها بالمقارنة مع سن قانون موحد يشمل جميع محاور القضاء السيبراني.

إلا أن لهذه المنهجية سيئات تتمثل في ضعف التنسيق والتلاؤم فيما بين القوانين المتعددة للفضاء السيبراني.

وبتعدد المرجعيات وغياب الفهم الشامل للموضوع ومفرداته وعدم التعاطي مع القضاء السيبراني على أنه بيئة واحدة وتجدر الإشارة إلى أن بعض البلدان ما يجري دمج المعاملات الإلكترونية والتجارة الإلكترونية تحت القانون نفسه، أو دمج المعاملات الإلكترونية مع التوقيع الإلكتروني، كما لجأت عدة أخرى إلى دمج قانون الجرائم الإلكترونية مع قانون المعاملات والتجارة الإلكترونية.

ولكن نحن نرى الأخذ بالمنهجية الشاملة المتمثلة في صياغة قانون إلكتروني (الشؤون الإلكترونية) واحد يغطي كافة محاور القضاء السيبراني، على غرار تجربة كل من جنوب أفريقيا وماليزيا، ويمكن تسمية هذا القانون الشامل بقانون تكنولوجيا المعلومات والاتصالات أو قانون المعلوماتية أو القانون السيبراني (كالقانون الماليزي) وبالرغم من صعوبة هذه المنهجية إلا أنها تضمن التغطية الشاملة لكافة مواضيع القضاء السيبراني، وتساهم في توحيد الإجراءات التنفيذية والاشرافية وخاصة إذا ما تم إقرار جهة تنفيذية واحدة لمراقبة تطبيق هذا القانون الشامل، كما تضمن التكامل والمواءمة بين الحلول القانونية والأحكام ضمن التشريع الواحد، ويجدر التنويه بمشروع قانون تكنولوجيا المعلومات اللبناني الجديد الذي يغطي عدة محاور هي التوقيع الإلكتروني، والمعاملات الإلكتروني، والجرائم الإلكترونية وحماية معالجة البيانات ذات الطابع الشخصي، وبالتالي فهـي أقرب ما يكون إلى قانون شامل للفضاء السيبراني.

وقد اعتمدت الإسكوا إلى حد كبير هذه المنهجية بوضع مجموعة متكاملة من القوانين تغطي ستة مواضيع للقضاء السيبراني، وتأمل الإسكوا أن تعتمد إرشاداتها في المنطقة العربية مما يؤدي إلى تعزيز تناسق القوانين بين البلدان العربية المختلفة وإتاحة وسائل التعامل والتبادل الإقليمي والدولي.

آليات صياغة واعتماد القوانين السيبرانية

تعطى عملية صياغة وإقرار القوانين في معظم البلدان العربية شعوراً واضحاً بالبطء الشديد وذلك لأسباب عديدة أهمها التسلسل الهرمي المعقد والتدخل السياسي الذي يلعب دوره أحياناً في تأخير مسودات القوانين

كما كان للحراك الاجتماعي والثورات العربية التي واكبت العقد الثاني من القرن الحالي وما آلت إليه ظروف بعض الدول من التفكك والتشرذم مما أدى إلى تعطل أو حتى توقف العملية التشريعية بكافة مراحلها وصورها من الصياغة إلى دراسة مشاريع القوانين وحتى إقرارها من قبل المجالس البرلمانية التي بات بعضها معطلاً تماماً.

كما بينت إحدى الدراسات التي قامت بها الإسكوا من لجوء عدد من البلدان العربية إلى الاعتماد على نماذج قوانين خارجية بعد ترجمتها، ما يؤدي إلى بعد التشريعات السيبرانية ذات الصلة بالمجتمع عن واقع المجتمع الذي تهدف لتنظيمه.

ويوجب ذلك ربط العملية التشريعية في مجال الفضاء السيبراني بالمجتمع المعني، لكي يتلاءم تطبيقها مع المجتمع وأعرافه.

وكثيراً ما يسود الشعور بغرابة تلك التشريعات عن الوسط القانوني الذي وضعت فيه، وقد يكون مرد ذلك حداثة المواضيع التي تتناولها أو سوء ترجمة وأقلمة القواعد القانونية المدرجة فيها مع النظام الوطني.

فالتجارب تشير إلى وجود صعوبات في ترجمة النصوص التقنية التي تأتي من الخارج كما تبين الدراسات بأن السلطات المختصة في البلدان العربية تسعى باسم الخصوصية المحلية وشخصية المجتمع إلى تحوير تلك التشريعات بعد ترجمتها بحيث تغلب فيها اعتبارات الحصر والمراقبة والمعاقبة على مبدأ حرية التواصل في الفضاء السيبراني.

كما توضح إحدى دراسات الإسكوا أن هذا اهتمام بعض البلدان العربية بموضوع تشريعي ما، قد لا ينطلق حكماً من حاجة وطنية بل من مؤثرات خارجة، مثل إقرار اتفاقيات دولية في موضوع ما، إذا نلاحظ تسارع بعض البلدان العربية إلى الالتزام بهذه الاتفاقيات بغض النظر عن أولويتها على المستوى الوطني.

عوائق تطبيق القوانين السيبرانية

يرتبط تطبيق القوانين بتوفر اللوائح التنفيذية والقرارات الإجرائية والأدوات التنظيمية اللازمة، ويشكل غياب بعض هذه المستلزمات التشريعية، أو مجملها عائقاً أمام تطبيق القانون وتفعليه ويلاحظ أن عدداً من البلدان العربية قد أقر قوانين خاصة بالمعاملات والتجارة الإلكترونية ومع ذلك فما زالت التجارة الإلكترونية

والمعاملات الإلكترونية محدودة الاستخدام نظراً لضعف الإجراءات والأدوات التنظيمية لها، مما أدى إلى ضعف في تطبيق هذه القوانين وفيما يأتي نسرد أهم العوائق المتعلقة بتطبيق وتنفيذ التشريعات السيبرانية وهي:

غياب أو ضعف الهياكل المؤسساتية

إن غياب أو ضعف فعالية معايير الانشاء أو الاختيار للهيئات التنظيمية والتنفيذية والرقابية الخاصة بالقوانين السيبرانية هي من العوائق الأساسية لتطبيق هذه القوانين، وتبين بعض التجارب في المنطقة العربية ضعف هذه الهياكل التنظيمية وقد تكون غير موجودة أصلاً في بعض البلدان كما أن بعض الهيئات ذات الصلة بتطبيق القانون قد لا توكل إليها المهام الأساسية التي تقوم بها الهيئات المماثلة في باقي مناطق العالم، مما يعيق تطبيق القوانين أيضاً.

غياب التعاون والتنسيق الإقليمي

إن غياب أو ضعف التنسيق الإقليمي والدولي في بعض المسائل التقنية الخاصة بالتشريعات السيبرانية خاصة تلك المتعلقة بالجرائم السيبرانية يعيق تطبيق هذه القوانين على المستوى الوطني.

الضوابط القضائية وضعف منظوماتها

يؤدي ضعف المنظومة القضائية وضوابط عملها التي تتضمن الكوادر المتخصصة والتجهيزات المادية والفنية والتقنية الملائمة إلى زيادة احتمالات عدم فعالية التشريع.

فالتطبيق العملي للتشريعات يتطلب معدات وأجهزة متخصصة وكوادر مؤهلة وتدريباً دائماً لهذه الكوادر على أحدث التقنيات وآليات لملاحقة حالات التعدي والإخلال وضبطها والتحقيق فيها ومن ثم إحالتها للقضاء ليفصل فيها تطبيقاً للقانون.

التدريب المستمر لأعضاء النيابة والقضاة

يتضح بجلاء ضعف وغياب التأهيل والتدريب المستمر لأعضاء النيابة والقضاء في مسائل التشريعات السيبرانية وكذلك غياب التخصصية في المحاكم، وضعف أداء المكاتب الفنية حيال تحليل الأحكام والمخرجات وتوثيقها ونشرها لتكون مادة متوفرة للباحثين ومراكز الدراسات، تشكل كلها عوائق إضافية أمام تطبيق التشريعات السيبرانية وتفعليها على أرض الواقع.

والله أسأل التوفيق والرشاد،

التوصيات

إن أهم ما يجب أن تنادي به ونوصي به في هذا المقام هو الحرص والحيطة على كافة المستويات وفي كل المجالات في التعامل مع الغير ومع كل ما يحيط بنا في مجال تكنولوجيا المعلومات ووسائل الاتصالات الحديثة.

ولقد عمدت الإسكوا خلال تنفيذ مشروع "تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية" إلى التعاون مع العديد من الخبراء والمنظمات الإقليمية المعنية بتطوير مجتمع المعلومات وإلى إشراك أصحاب المصلحة المعنيين بتطوير التشريعات السيبرانية في المنطقة العربية.

ولعل أهم ما جاءت به كافة الاجتماعات والمؤتمرات التي تمت قبل كتابة هذا البحث، وأغلب ما تم التوصية به من المناقشات قسمناها إلى خمسة محاور رئيسية وهي:

- توصيات للحكومات حول صياغة واستكمال التشريعات السيبرانية.
- توصيات حول العملية التشريعية.
- توصيات حول وضع التشريعات السيبرانية موضع التنفيذ.
- توصيات خاصة بالبعد الإقليمي.
- توصيات حول التوعية والتدريب والتعليم.

وهي تفصيلاً كالآتي:

1. توصيات للحكومات حول صياغة واستكمال التشريعات السيبرانية

يجب التأكيد على مدى أهمية إنشاء وتحديث منظومة شاملة للتشريعات السيبرانية لتتلائم مع احتياجات البيئة الرقمية وتطبيقاتها، وتسمح بحماية المستخدم وتمكن من بناء الثقة باستخدام الفضاء السيبراني وخدماته.

حيث المدخل الرئيسي لإيجاد بنية تشريعية وتنظيمية فاعلة للفضاء السيبراني في العالم العربي وخاصة دول مجلس التعاون الخليجي هو إيجاد الإطار الإشرافي الشامل والمتخصص الذي ينطلق في عمله من استراتيجية واضحة الأهداف والآليات لمواجهة التحديات على الصعيد الوطنية في كل بلد حيث في ذلك لا بد من مسارين:

الأول: الإقرار بما هو قائم والعمل به دون تغيير جوهري.

الثاني: إحداث تغيير شامل نحو عالم تكنولوجي متين وأمين وأكثر أماناً وهو المسار الأفضل والأكثر فاعلية.

ولأجل ذلك نتصور لذلك ثلاثة اتجاهات تتيح للدولة مواجهة المعوقات والتحديات القائمة على الصعيد الوطني أمام تطبيق التشريعات السيبرانية التي سبق الحديث عنها، وتحديداً عائق تعدد الجهات والهيئات المنوط بها التشريع والتنفيذ والتطبيق المباشر والغير مباشر ولأجل تباين المخرجات تبعاً لذلك وهذه الاتجاهات هي:

الاتجاه الأول:

إيجاد هيئة واحدة منوط بها تحديث البنية التشريعية القائمة للفضاء السيبراني عبر تقييم التشريعات القائمة، واقتراح التعديلات والتدابير التي تسد النقص، وضمان التنسيق بينها، حيث فاعلية هذا الاتجاه تقوم على إيجاد تشريع واحد متناسق للفضاء السيبراني أو لأكبر مجموعة مسؤولة عن السياسات والبنى التشريعية وتقليص الأطر التنظيمية والتنفيذية إلى أبعد مدى طالما أنها ستكون قادرة على القيام بواجبات التنظيم المحكومة بالتشريع الواحد أو ما تفرع عنه وتكامل معه، ويتطلب هذا الاتجاه تغييراً جوهرياً على الأغلب، وهو الخيار الأفضل الذي تحييه التدخل التشريعي لإيجاد قانون يمكن أن يكون عنوان قانون تكنولوجيا المعلومات والاتصالات أو قانون الفضاء السيبرانية الموحد.

الاتجاه الثاني:

إيجاد إطار تنسيقي واحد يتضمن سائر الجهات والهيئات القائمة المعنية بالبنية التشريعية السيبرانية واحتياجات سد النقص فيها وتنسيق تشريعاتها وتطبيق مشاريعها.

إن هذا الاتجاه يقر بتعددية هيئات التشريع، لكنه يعيد ترتيبها ضمن إطار تنسيقي، وليس إطار إشرافي وتنظيمي واحد لجهة إعادة بناء التشريع بما يخدم موضوعياً وإجرائياً سائر فروع ومسائل الفضاء السيبراني، ولا يؤدي هذا الاتجاه حكماً إلى وضع تشريع واحد للفضاء السيبراني بل يؤدي إلى وضع حزمة متناسقة من التشريعات ولعل هذا الاتجاه ولعل هذا الاتجاه يلائم العالم العربي.

الاتجاه الثالث:

وهو الذي يفرضه غياب القرار الحكومي بالإطار التنسيقي أو عدم الثقة بقدرة الأطر القائمة على تحقيق الأغراض المرجوة أو يستعاض عنه بتولي الجهة التشريعية في الدولة أو الحكومة إطلاق مشروع تقييم

التشريعات السيبرانية القائمة على الصعيد الوطني، واقتراح مشاريع التعديلات ومشاريع التدابير الجديدة والتي تلائم المجتمع وخطط تطبيق المخرجات.

ويتناسب مع هذا الخيار أو الاتجاه إسناد تنفيذ هذا المشروع إلى فريق الخبرة الملائم ثم طرحه للبحث والمراجعة بمشاركة إلزامية لكل الهيئات المعنية لعرض آرائها، والتقدم بالمخرج النهائي لجهات صناعة القرار، ومهما كانت الاتجاهات المعتمدة فإن صياغة القوانين وخاصة التي تعالج الأمن المعلوماتي والسيبراني تتطلب:

- قيام الجهة التشريعية بتقييم التشريعات السيبرانية القائمة على الصعيد الوطني عبر دراسات بحثية معمقة لتحديد مواضع النقض والآليات المثلى لإيجاد الحلول وتطبيقها، ويحتاج ذلك إلى فريق عمل متخصص، وإلى إشراك الوزارات والهيئات المعنية للمراجعة والموافقة على هذه الدراسات.
- إنشاء لجان متخصصة لوضع مسودة القانون تتضمن خبراء في المجال القانوني ومجال تكنولوجيا المعلومات والاتصالات، كما يفضل أن تتضمن ممثلين عن الهيئات المتخصصة من المجتمع المدني والقطاع الخاص.
- الاستعانة بالاتفاقيات الإقليمية والدولية المرتبطة بتشريعات الفضاء السيبراني وذلك لضمان تناسق التشريعات الوطنية معها.

ونحن في هذا الصدد نادي بالانضمام إلى مثل هذه الاتفاقيات في حال تلاؤمها مع حاجة مجتمعاتنا وتتماشى مع طبيعتنا وثقافتنا والاحتياجات والأولويات الوطنية ويمكن الاستعانة أيضاً بإرشادات الإسكوا المتكاملة للتشريعات السيبرانية والتي تغطى كافة مواضيع الفضاء السيبراني بالإضافة إلى موضوع حق الوصول إلى المعلومات وحق مهم لبناء مجتمع المعلومات.

2. توصيات عند إقرار تشريعات في المجال السيبراني

يتطلب التشريع في المجال السيبراني والأمن المعلوماتي توفر خبرات متنوعة وتحديداً في مجالي القانوني وتكنولوجيا المعلومات والاتصالات، كما يتطلب الأخذ بعين الاعتبار جميع حاجات ومتطلبات القطاعات المختلفة الحكومية منها وكذلك القطاع الخاص، وقطاعات المجتمع المدني كالاتحادات والنقابات.

لذلك، ينبغي توفير الظروف التي تجعل التشريع منبثقاً من المجتمع نفسه الذي يهدف لتنظيمه، بل أن يكون منقولاً عن تشريعات خارجية قد لا تعكس الوضع والثقافة والبيئة التي تميز المجتمعات العربية التي ما زالت تأخذ بالعادات والتقاليد وتحافظ على القيم الدينية السماوية وترفض الانفتاح اللاأخلاقي.

لذا يجب من أجل موضوع التشريعات السيبرانية في المنطقة العربية حيث قلة الخبرة وحداثة التشريعات في هذا المجال يمكن أن نقترح ما يلي:

- **تعزيز شفافية العملية التشريعية أثناء إعداد القوانين ومناقشاتها وكذلك نفس الشيء عند إقرارها:**

وذلك من خلال توسيع دائرة لجان إعداد التشريعات لتضم أصحاب المصلحة والأطراف المعنية كافة، أي الوزارات والمؤسسات الحكومية ومؤسسات المجتمع المدني والشركات الخاصة كمقدمي الخدمات عبر شبكة الانترنت وجمهور المستهلكين، بدل أن تقتصر على الخبراء والمستشارين الخارجيين فقط.

- **تسجيل وحفظ كافة المداولات الخاصة بلجان الصياغة:**

وذلك بشكل كامل وواضح وقابل للبحث العلمي والمناقشة المجتمعية والأخذ بكل الآراء لما في ذلك من فائدة في تفعيل النصوص التشريعية بعد إقراراها.

- **تطوير أساليب البحث الميداني أثناء العملية التشريعية:**

وذلك لأن من أهداف البحث الميداني المنظم لتسجيل أنماط السلوك والتعاملات والعقود والممارسات الحميدة للمتعاملين عبر الفضاء السيبراني وتصوراتهم حول طرق العمل في هذا الفضاء للاستفادة منها أثناء التشريع وإلى تحديد الممارسات التي لا تتناسب وحاجة وقيم المجتمعات العربية ومعالجتها بالتشريعات الملاءمة، حيث يتطلب البحث الميداني الاستعانة بالباحثين في علم الاجتماع والذين تتوفر لديهم أدوات الملاحظة والبحث الميداني، كإجراء الإحصاءات والاستقصاءات والمقابلات الشخصية والجماعية.

- **ضرورة تنسيق النصوص التشريعية ضمن الدولة:**

وذلك تفادياً لأي تكرار أو تناقض محتمل بين تشريعات الفضاء السيبراني والقوانين النافذة الأخرى، فالتشريعات الخاصة بالمعاملات الإلكترونية وإن كانت حول علاقات تتم عن بعد وعبر الوسائط الإلكترونية قد تتضمن تكراراً لنصوص القواعد العامة المنظمة للعقود أو الاثبات لجهة آلية انعقاد العقود أو حجية المحررات، وقد يؤدي التناقض بين النصوص التشريعية إلى مشاكل في التطبيق، مع احتمال نشوء حالات عدم فعالية النصين (النص الجديد، الخاص بالفضاء السيبراني، والنص القديم العام)، وبالتالي من المهم إصدار قائمة تحت كل مادة من مواد التشريع الجديدة سواء بالتعديل أو الإلغاء.

- **تشجيع إصدار المذكرات الإيضاحية:**

وذلك لأنها تتضمن تعليقات رسمية عن كل مادة من مواد التشريع وتأتي المذكرة الإيضاحية بعد إتمام المداولات في التشريع وإصدار القانون من قبل الجهة التشريعية المخولة بذلك.

كما تتضمن المذكرة الإيضاحية ملخصاً بمداولات لجان الصياغة وتعليقاً على كل مادة من مواد التشريع المزمع إصداره، حيث يحتوي على بيان بالسياسة التشريعية التفصيلية للنص المعني، والمصالح التي يرغب المشرع بصيانتها أو الموازنة بينها في النص التشريعي وكذلك نطاق تطبيقه.

- **الاهتمام بالاجتهادات القضائية:**

وذلك من خلال إجراء بحوث علمية عنها وحولها وإعداد دراسات لمقارنة الاجتهادات الصادرة في بلدان المنطقة وفي بعض البلدان المتقدمة.

- **طرح النصوص الأولية لتشريعات الفضاء السيبراني للاستشارات العامة:**

وذلك من خلال تشجيع النقاش العام حولها، عبر الوسائل الإلكترونية المتعددة التي تتيح تبادل الملاحظات والمشاركات حول نص القانون، أو من خلال الدعوة لورش عمل أو ندوات وطنية بمشاركة كافة الأطراف المعنية لضمان نقاش عام متوازن وفعال.[2]

- **تشجيع المنظمات غير الحكومية العاملة في مجال التشريعات**

وذلك من خلال تشكيل مجموعات عمل تساهم في حث الحكومات والمجالس التشريعية على تطوير القوانين الخاصة بالفضاء السيبراني.

3. توصيات حول التشريعات السيبرانية

موضع التنفيذ

وتهدف هذه التوصيات الخاصة بوضع التشريعات السيبرانية موضع التنفيذ إلى التركيز على آليات تفعيل التشريع بعد إقراره وتفاعله مع المجتمع الذي يتوجه إليه، وذلك من خلال النقاط والآليات الآتية:

---

[2] عن د/ عبد الفتاح بيومي حجازي، النظام القانوني للتوقيع الإلكتروني (دراسة تأجيلية مقارنة) المجلة للكتب القانونية 2007 ص 331 وما بعدها، كذلك د/ سامي شرف، الاختلافات الأساسية في تشريعات المعاملات الإلكترونية في بلدان الإسكوا، نشرة تكنولوجيا الاتصالات للتنمية في غرب آسيا، الإسكوا، العدد 11 وثيقة الأمم المتحدة (EIESCWA/ICTD/2009) ص 11، 14 وما بعدها.

أ) آلية حث الحكومات على وضع لوائح وإجراءات تنفيذية للتشريعات السيبرانية، وإيجاد البنى التحتية الضرورية لتطبيق هذه التشريعات مع تأمين التمويل اللازم لها، ويمكن تبنى أحد الخيارين التاليين من أجل إيجاد البنى التحتية التنظيمية الضرورية لتطبيق التشريعات السيبرانية وذلك من خلال:

- إنشاء هيئة عليا واحدة مسؤولة عن تشريعات الفضاء السيبرانية واللوائح التنفيذية لها ويجري إنشاء هذه الهيئة من خلال تدبير تشريعي خاص يأخذ بعين الاعتبار البنى التنظيمية القائمة ويضمن التنسيق فيما بينهما ويقترح التعديلات اللازمة عليها، ويعد هذا الخيار الأشمل والأمثل إلا أنه قد يتطلب تغيرات جوهرية صعبة البلوغ في بعض البلدان.
- وضع إطار للتنسيق بين الجهات الحكومية وذلك لتفادي الازدواجية في صياغة وتطبيق التشريعات، وسد مكامن النقص فيها، ويبقى هذا الخيار على تعددية الجهات المسؤولية عن التشريع السيبراني، إلا أنه يحتاج إلى قرار رسمي يضمن التزام كافة الجهات المعنية، مع تحديد مجال عمل ومسؤوليات كل منها وآليات التعاون في المشاريع والبرامج المشتركة.

ب) آلية إعداد دراسات جدوى اقتصادية خاصة بتأمين الموارد التمويلية للبنى التنظيمية الخاصة بالتشريعات

إذا أن تأمين الموارد اللازمة للتشريع هي من أهم المواضيع التي يجري بحثها داخل الهيئات الدستورية المعنية في كل البلدان العربية ويجري في هذا الصدد بحث إمكانية التمويل الذاتي للهيئة التنظيمية من خلال عوائد الترخيص أو منح الموافقات وغيرها، أو الاعتماد وعلى مخصصات من الموازنة العامة للدولة أو المزج بين الوسيلتين كما يطرح في هذا المجال موضوع الموارد المالية لتلك الهيئات وذلك من خلال الإجابة عن ما يلي:

هل تحتفظ بها، كلياً أو جزئياً، أم تحولها إلى الجزئية العامة للدولة المعنية؟

وكيف تغطى التكاليف عن وقوع عجز في إحدى السنوات المالية؟

جـ) تأهيل الكوادر التنظيمية والعدلية المناسبة

وذلك من خلال تنمية المعرفة لدى الكوادر الإدارية المعنية بتطبيق القانون، بأفضل الممارسات المتبعة عالمياً في مجالات الفضاء السيبراني، إضافة إلى السياسات والقواعد والإجراءات المعتمدة في التشريع، بما من شأنه أن يزيد من فعالية التشريع في المجتمع الذي يتوجه إلى تنظيمه.

د) وضع الحلول التشريعية بحيث تكون منسجمة مع الواقع الحياتي

وذلك بما يتلاءم مع وجهة نظر المجتمع وذلك بعد الوقوف علـى طبيعة وأنماط العلاقات السائدة فيه، مما يؤدي إلى فعالية أكبر في تطبيق القانون.

هـ) تخفيض الموارد المالية والبشرية لإجراء البحوث الميدانية لتسجيل وتوصيف الممارسات السائدة على الصعيد الوطني

وذلك في مجالات الفضاء السيبراني المختلفة، مما يمكن المشرع من رصد تفاعل التشريع مع المجتمع وتحديد الإجراءات التشريعية المطلوبة للتعامل مع الواقع القانوني السائد.

4) توصيات حول البعد الإقليمي

وتبرز أهمية التعاون والتنسيق الإقليمي على المستويين العربي والدولي في العملية التشريعية وفي تطبيق القانون نظراً للطبيعة الشمولية للفضاء السيبراني، ولأهمية التنسيق بين البلدان العربية ومجلس التعاون الخليجي بصفة خاصة وذلك من أجل المجانسة فيما بين التشريعات السيبرانية ودفع عملية التكامل الإقليمي لبناء مجتمع معرفة عربي، وتسهيل عملية التنسيق الإقليمي بين التشريعات السيبرانية بشكل خاص في الاعتراف بالدليل الرقمي إقليمياً وفي تحفيز المعاملات الإلكترونية وخاصة التجارية منها، بين بلدان المنطقة كما تساهم بشكل كبير في مكافحة الجريمة الإلكترونية وفي تسهيل تتبع آثار الجريمة الإلكترونية على صعيد المنطقة.

وتجدر الإشارة إلى أن اعتماد قوانين متلائمة في مجال الملكية الفكرية ضمن الفضاء السيبراني ومناسبة للوضع الاقتصادي والاجتماعي والثقافي في دول المنطقة العربية ودول الخليج خاصة، حيث يعتبر هذا أحد العوامل التي تساعد في بناء الاقتصاد المبني على المعرفة إقليمياً ويبرز هنا دور المنظمات الإقليمية والعالمي والعمل المستمر لزيادة التجانس بين التشريعات السيبرانية في المنطقة العربية.

5) توصيات حول التوعية والتدريب والتعليم

- وذلك من خلال يكتسب موضوع بناء القدرات أهمية كبـرى في شتى المجالات وللوصول إلى التطبيق الأمثل للقوانين وبناء منظومة متكاملة تعنى بشؤون الفضاء السيبراني بما فيها من مؤسسات وعاملين، يجدر إيلاء عناية خاصة للتوعية والتدريب والتعلم على كافة الأصعدة لضمان الفهم والوعي بمشتملات القوانين السيبراني وآليات تطبيقها.

- لذا نوصي بتنظيم مجموعة متنوعة من ورش العمل والندوات الوطنية ووضع تصورات متخصصة من خبراء متخصصين ولا بد أن يندرج ذلك تحت مشروع وطني شامل بدلاً من أن تكون مجرد أنشطة متفرقة.
- كذلك تنظيم ورش عمل خاص بالجهات والهيئات البرلمانية والتشريعية حول أهمية التشريعات السيبرانية لبناء الثقة بالفضاء السيبراني وبالخدمات الإلكترونية وحماية المستخدم.
- إعداد تدريب موجه ومخصص للقضاة والمحامين على صياغة قوانين وتشريعات تتلاءم مع مستلزمات الفضاء السيبراني.
- إقامة ورش عمل تدريبية وطنية للفنيين وأعضاء النيابة العامة والأجهزة الأمنية ورجال الضبط القضائي حول نصوص التشريعات السيبرانية وكيفية تطبيقها حماية للفرد والمجتمع والأمن الوطني وكذلك الأمن القومي.
- عقد اجتماعات عمل وطنية وإقليمية للخبراء في مجال الفضاء السيبراني لتبادل التجارب والخبرات الجديدة في المجال.
- تنفيذ برامج لتأهيل أجهزة الضبطية القضائية من خلال توفير كوادر تتمتع بمعرفة تخصصية وإتاحة الوسائل التقنية اللازمة لها.
- إقامة برامج التوعية لفئات المجتمع وأفراده لمعرفة كيفية حماية نفسه وأسرته ومجتمعه من الجرائم الإلكترونية السيبرانية وتبصيره بالتشريعات السيبرانية وأهميتها في ضمان حماية المستخدمين للفضاء السيبراني.
- تطوير نظم التعليم من مناهج وطرق تدريس ومعلم وأدوات التعليم لتواكب العصر وهذا ما جعلنا نذهب إليه مضطرين خاصة تحت ظروف كوفيد 19 وما فرضته على العالم من التعليم عن بُعد أو أونلاين.
- كما يجب إدخال المواضيع المتعلقة بالتشريعات السيبرانية في مناهج كليات تكنولوجيا المعلومات والاتصالات لدراسة الجانب القانوني.
- تضمين مناهج كليات الحقوق والدراسات العليا القانونية التشريعات والقوانين والجرائم السيبرانية لتخريج جيل واعي بأهمية هذه الجرائم ومدى أثرها على المجتمع وعلى مرفق العدالة.
- إقامة دروات خاصة لربات البيوت والسيدات وخاصة الفئة التي تقيم بالمنزل أطول فترة لارتباطها بالفضاء السيبراني ولتبصيرها بمخاطر الإفراط في استخدام الفضاء السيبراني صحياً واجتماعياً وأمنياً

وعرض للجرائم الحادثة ومدى تدميرها للعلاقات الأسرية وكيفية وضع الانسان نفسه تحت طائلة القانون.

والله ولي التوفيق،،،

La protection juridique des données à caractère personnel des salariés

Khadija ANOUAR
Enseignante-chercheuse à la Faculté des Sciences Juridiques
Economiques et Sociales de Fès
Université Sidi Mohamed Ben Abdellah

Résumé :

Le cadre juridique marocain des données à caractère personnel englobe différents textes de lois, le plus important est la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. La protection de la vie privée de la personne constitue un droit primordial reconnu par la déclaration universelle des droits de l'Homme de l'Organisation des nations unies datant du 1948 qui prévoit dans son article 3 « *Tout individu a droit à la vie, à la liberté et à la sureté de sa personne* ».

Au niveau institutionnel, la commission de protection des données personnelles propose à son tour des mesures qui visent à protéger et conserver les données des personnes.

Le problème juridique posé consiste à aborder le cadre juridique réglementant les données personnelles et d'élucider les lacunes et insuffisances juridiques et institutionnelles que rencontre notre législation en vigueur et en deuxième lieu nous allons présenter des propositions pour faire évoluer notre droit positif tout en illustrant avec d'autres systèmes étrangers assez développés en la matière.

Mots clés : Droit, protection, données à caractère personnel, données privées, salariés.

Abstract :

The Moroccan legal framework for personal data encompasses various legal texts, the most important of which is Law No. 09-08 on the protection of individuals with regard to the processing of personal data. The protection of the private life of the person constitutes a fundamental right recognized by the Universal Declaration of Human Rights of the United Nations Organization dating from 1948 which provides in its article 3 “Everyone has the right to life, to freedom and security of person”.

At the institutional level, the personal data protection commission in turn proposes measures aimed at protecting and preserving personal data.

The legal problem posed consists of addressing the legal framework regulating personal data and clarifying the legal and institutional gaps and inadequacies encountered by our current legislation and secondly we will present proposals to develop our positive law while illustrating with other fairly developed foreign systems in this area.

Keywords : Law, protection, personal data, data privacy.

Introduction :

Dans notre monde digitalisé, l'offre d'informations est devenue une réalité phénoménale vécue au quotidien[3].

Les données à caractère personnel des salariés sont parfois perçues comme étant des informations neutres, partageables sans précaution sur un site web, à la banque, lors de souscription d'un contrat d'assurance, chez le médecin de travail, ou que l'on donne ses coordonnées à une administration, ce simple acte n'est pas toujours sans conséquence[4].

En fait, la Suède était le premier pays à formuler une loi pour la protection des données personnelles en 1974, en France c'est la loi informatique et liberté de 1978.

Au Maroc, la protection des données à caractère personnel est assurée par la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel adoptée en février 2009, qui porte aussi l'obligation pour les employeurs de tout mettre en œuvre pour garantir la protection des données de leurs salariés.

La commission nationale de contrôle de la protection des données personnelles est instituée comme autorité chargée de la protection des données personnelles, elle vérifie les traitements de données et accompagne les institutions publiques et privées en vue de se mettre en conformité avec la législation.

Toutefois, la protection des données personnelles des salariés ne doit pas freiner l'innovation, mais l'encourager et la favoriser. Elle ne doit pas être non plus un alibi pour masquer la fraude, et remettre en question les équilibres recherchés. Au contraire, elle doit mener vers la confiance numérique.

Ceci dit que certaines questions demeurent légitimes, des questions pour le salarié qui ne sait quoi faire relativement à la caméra installé dans les milieux du travail, suite à la publication de photos ou de vidéos, à la réception d'un message intrusif ?

3- BENSOUSSAN Alain, *La protection des données personnelles de A à Z,* éd., Bruylant, 2017, p. 56.
4- LAFFAIRE Marie-Laure, *Protection des données à caractère personnel tout sur la nouvelle loi*, éd., Eyrolles, 2005, p. 43.

Et puis encore des questions pour les responsable de traitement des données à caractère personnel, si l'on savait que l'instruction des notifications et des dossiers prend du temps, quelle démarche entreprendre pour se mettre en conformité et comment savoir si un dispositif technologique est déplorable ?

Si la protection des données à caractère personnel, de la vie privée et de la confiance numérique, et l'impératif économique ont justifié la nécessité de réglementer la protection des données à caractère personnel sur le plan interne comme un impératif d'adéquation de la législation nationale avec les principes relatifs aux droits humains énoncés dans des textes fondamentaux internationaux et nationaux[5].

La protection des données personnelles des employés représente à la fois un sujet essentiel en entreprise et une inquiétude de la part des salariés.

Cependant quelles sont les obligations de l'employeur concernant la protection des données personnelles de ses salariés ? Et quels sont les droits des salariés vis-à-vis de leurs données personnelles ? Quelles règles les employeurs doivent-ils respecter en termes de protection des données personnelles ? Quels sont les droits des employés ?

Si la légitimité de la protection des données à caractère personnel des salariés est une exigence sociétale et économique, comment le Maroc envisage-t-il contribuer tout en conciliant le respect de la vie privée des salariés, l'innovation et l'intérêt public ? C'est ce que nous allons démontrer en abordant le cadre juridique de la protection des données personnelles des salariés et traiter ensuite des mesures de propositions pour une meilleures protection.

I- L'aspect juridique de la protection des données personnelles des salariés

Le droit au respect de la vie privée est un droit humain fondamental. D'après l'article 24 de la Constitution marocaine de 2011 qui dispose que : « *Toute personne a droit à la protection de sa vie privée* ». La vie privée des salariés doit être protégée contre toutes les atteintes qui peuvent l'affecter, notamment celles qui portent sur leurs informations personnelles dans les milieux du travail.

5- DESGENS-PASANAU Guillaume, *La protection des données à caractère personnel*, éd., Lexis Nexis, 2018, p. 76.

A- L'encadrement juridique des données personnelles des salariés

La nécessité de réglementer la protection des données à caractère personnel a été une nécessité afin de préserver les données personnelles des individus dont également les salariés.

1-Cadre juridique des données des salariés

Les entreprises sont de plus en plus tenues d'assurer la protection des données personnelles. Aussi, tout organisme privé qui collecte un certain nombre de données personnelles sur ses salariés se doit de les protéger.

Les données à caractère personnel sont constituées de toutes les informations anonymes dont le recoupement permet d'identifier une personne précise (par exemple, une emprunte digitale, l'ADN…) Il peut s'agir, soit du patronyme, soit du numéro de sécurité sociale, soit du numéro d'immatriculation d'un véhicule automobile et plus généralement de toutes données qui, sans avoir un rapport direct (nom, prénom, adresse, situation familiale...), permettent d'établir un lien avec le salarié concerné[6]. Il est à recommander que la législation prévoie une définition juridique spécifique des données personnelles à caractère professionnels.

Gestion des recrutements, gestion de la paie, la vidéosurveillance sur le lieu de travail, le système des cartes biométrique pour contrôler l'accès aux locaux, la cyber surveillance… sont autant de pratiques technologiques mises en place par l'entreprise et qui risquent de porter atteinte aux droits des salariés[7].

En vertu de la loi n°09-08 du 18 février 2009 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel[8] énonce les faits qui constituent des infractions. Nous les résumons comme suit :

- Tout traitement portant atteinte à l'ordre public, à la sureté, à la morale et aux bonnes mœurs ;

6- METILLE Sylvain, *Protection des données*, éd., Helbing Lichtenhahn Verlag, 2019, p. 59.
7- LE GUYADER Patrick, *Protection des données sur internet*, éd., Lavoisier, 2013, p. 47.
8- Loi n° 09-08 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel; Bulletin Officiel n° 5744 du 24 joumada II 1430 (18 juin 2009).

- La mise en œuvre d'un traitement sans l'autorisation ou la déclaration exigée, Le refus du droit d'accès, de rectification ;
- Toute incompatibilité avec la finalité déclarée ;
- Le non-respect de la durée de conservation des données ;
- Le non-respect des mesures de sécurité des traitements ;
- Le non-respect du consentement de la personne concernée ;
- Toute entrave à l'exercice des missions de contrôle de la Commission Nationale de Données à Caractère Personnel (CNDP) ;
- Tout refus d'application des décisions de la CNDP.

Dans un contrat de travail, l'employeur collecte et traite les données personnelles du salarié en vue d'assurer la gestion administrative de son dossier (paie, gestion de carrière).

Afin de permettre à l'employeur de répondre à ses obligations légales, ces données peuvent être transmises aux organismes de la prévoyance sociale (la CNSS, la CIMR,..) au service des impôts et aux compagnies d'assurance.

Ce traitement a fait l'objet d'une déclaration / demande d'autorisation auprès de la CNDP sous un numéro.

Le salarié peut s'adresser à la CNDP pour exercer ses droits d'accès, de rectification et d'opposition conformément aux dispositions de la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Quelles sont les obligations de l'employeur concernant la protection des données personnelles de ses salariés ?

L'employeur qui exploite des données personnelles est tenu respecter plusieurs obligations qui sont :

- Recueillir l'accord du salarié concerné ;
- Informer le salarié concerné de son droit d'accès, de modification ;
- Il doit veiller à la sécurité des systèmes d'information ;
- Il doit assurer la confidentialité des données personnelles ;
- Il doit assurer une durée de conservation des données personnelles.

L'objectif de la collecte d'informations doit être précis et les données doivent être partagées en accord avec cette finalité[9].

En ce qui concerne les données qui présentent un risque élevé pour les droits et les libertés des salariés, l'employeur devrait être tenu de mettre en place une analyse d'impact sur la vie privée pour évaluer l'origine, la nature et la gravité de ce risque.

La législation s'applique à toute entreprise établie sur le territoire marocain qui y effectue un traitement de données à caractère personnel. Seules les personnes physiques dont des données personnelles sont collectées bénéficient de la protection de la législation.

2- Les conditions et modalités de collecte des données à caractère personnel des salariés

L'employeur est amené à collecter des informations concernant ses salariés afin de procéder aux recrutements, calculer les horaires de travail ou encore établir la fiche de paie. Toutefois, la collecte de ces informations est strictement encadrée.

Les données des salariés collectées doivent avoir des **finalités** précises et légitimes que l'employeur convient de justifier précisément. Par exemple, la collecte des photos des salariés pour alimenter l'annuaire de l'entreprise.

Quelles sont ces règles à respecter ?

Les données des salariés doivent être collectées en respectant le consentement du salarié concerné, d'après les dispositions juridiques de l'article 5 de la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, la collecte et le traitement de données personnelles s'effectue qu'en ayant de la personne son consentement d'une façon claire, libre et avertie.

9- BANCK Aurélie, *RGPD : la protection des données à caractère personnel*, 3éme éd., Gualino, 2018, p. 38.

Tout salarié sollicité directement, en vue d'une collecte de ses données personnelles, doit être préalablement informée de manière expresse, précise et non équivoque par le responsable du traitement[10] ou son représentant.

Le consentement du salarié concerné c'est toute manifestation de volonté, libre, spécifique et informé, par laquelle la personne concernée accepte que les données à caractère personnel la concernant fassent l'objet d'un traitement (article 4 de la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel).

Les données des salariés doivent être traitées loyalement, licitement et conservées pour une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées.

Ces données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédent pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement.

En pratique, il peut s'avérer difficile de définir une durée d'où la nécessité que la législation prévoit une durée raisonnable de trois mois.

De plus, sur demande du responsable du traitement et, s'il existe un intérêt légitime, la commission nationale peut autoriser la conservation de données à caractère personnel à des fins historiques, statistiques ou scientifiques

Il est judicieux que tous les organismes qui traitent des données personnelles aient pour obligation de tenir un registre de traitement des données

---

10- Voir article 34 du décret n° 2-09-165 du 25 joumada I 1430 (21 mai 2009) pris pour l'application de la loi n° 09-08 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel; Bulletin Officiel n° 5744 du 24 joumada II 1430 (18 juin 2009), p. 1006.
Article 34 : « *1) Les informations à fournir par le responsable du traitement, en application de l'article 5 de la loi n° 09-08 susvisée, peuvent être délivrées par tous moyens, notamment par :*
-courrier électronique ou sur support papier ;
-affichage ou formulaire électronique ;
-annonce dans un support approprié ;
- ou bien, au cours d'un entretien individuel.
2) les codes, sigles et abréviations figurant dans les documents délivrés par le responsable de traitement en réponse à une demande doivent être explicités, si nécessaire sous la forme d'un lexique.»

personnelles. Et que les entreprises de moins de 100 salariés devraient seulement inscrire au registre :

- Les traitements de données non occasionnels ;
- Les traitements de données susceptibles de comporter un risque pour les droits et libertés des salariés ;
- Les traitements qui portent sur des données sensibles.

B-La mise en œuvre du traitement des données à caractère personnel

Le cadre juridique relatif à la protection des données personnelles renforce les droits de chaque salarié sur la protection de ses données personnelles et responsabilise les acteurs traitant ces données.

1- Régime de déclaration des traitements des données personnelles

Tout traitement doit faire l'objet d'une notification auprès de la commission nationale de contrôle de la protection des données à caractère personnel sous la forme d'une déclaration préalable ou d'une autorisation préalable selon la nature des données.

Cette déclaration a pour objet de permettre à la commission nationale d'exercer les compétences qui lui sont dévolues par la législation, afin de contrôler le respect de ses dispositions et d'assurer la publicité du traitement des données personnelles.

Aux termes des dispositions juridiques de l'article 14 de la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, le responsable du traitement ou, le cas échéant, son représentant doit adresser une déclaration à la Commission nationale préalablement à la mise en œuvre d'un traitement entièrement ou partiellement automatisé ou d'un ensemble de tels traitements ayant une même finalité ou des finalités liées[11].

11- Article 34 de la décision du premier ministre n° 3-33-11 : « *En application de l'article 14 de la loi n° 09-08, lorsqu'un ensemble de traitements relève d'un même organisme et a des finalités identiques ou liées entre elles, une déclaration commune devra être présentée suivant un modèle défini par la Commission, comportant les informations nécessaires propres à chaque traitement et, chaque entité concernée le cas échéant*.»

La déclaration doit comprendre :

le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant ;

la dénomination, les caractéristiques et la ou les finalités du traitement envisagé ;

une description de la ou des catégories de personnes concernées et des données ou des catégories de données à caractère personnel s'y rapportant ;

les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées ;

les transferts de données envisagés à destination d'Etats étrangers ;

la durée de conservation des données ;

le service auprès duquel la personne concernée pourra exercer, le cas échéant, les droits qui lui sont reconnus par les dispositions de la présente loi, ainsi que les mesures prises pour faciliter l'exercice de ceux-ci ;

une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la confidentialité et la sécurité du traitement ;

les recoupements, les interconnexions, ou toutes autres formes de rapprochement des données ainsi que leur cession, sous-traitance, sous toute forme, à des tiers, à titre gratuit ou onéreux.

Aux termes des dispositions juridiques de l'article 19 de la loi n°09-08, la commission nationale délivre, dans un délai de 24 heures courant à compter de la date du dépôt de la déclaration[12], un récépissé de ladite déclaration, dont les caractéristiques doivent figurer dans toutes les opérations de collecte ou de

---

12 - Article 26 du décret n°2-09-165: « *Lorsque la déclaration satisfait aux prescriptions de la loi n° 09-08 et de ses textes d'application. La CNDP délivre le récépissé prévu à l'article 19 de la loi susvisée. La CNDP peut délivrer le récépissé de la déclaration préalable par voie électronique avec accusé de réception par la même voie. Lorsque le récépissé est délivré par voie électronique, le responsable du traitement peut en demander une copie sur support papier*.»

transmission des données. Le responsable du traitement peut mettre ledit traitement en œuvre dès réception dudit récépissé.

2- Droits des salariés sur leurs données

Les salariés lors de la collecte de leurs données doivent être informés notamment de l'identité du responsable du traitement, des finalités du traitement, des destinataires des données, de l'existence d'un droit d'accès et d'un droit de rectification, ainsi que des caractéristiques du récépissé de la déclaration auprès de la CNDP ou de l'autorisation préalable.

Les personnes concernées ont également le droit de s'opposer au traitement pour des motifs légitimes. Ces informations doivent être mentionnées sur tout support destiné à recueillir des données personnelles[13].

Concernant le droit d'accès et de rectification, le salarié doit pouvoir avoir accès à ces données ainsi qu'à certaines informations sur leur traitement mais il est à constater qu'un délai devrait être prévu d'un mois.

Le droit de rectification par le salarié qui doit pourrait modifier par exemple son adresse en cas de déménagement.

Pour le droit d'opposition, la CNDP regarde de près si la procédure de droit d'opposition est respectée par les entreprises. Une personne physique peut s'opposer à la collecte de ses données réalisée à des fins de prospection, ou au titre de l'intérêt légitime de l'entreprise. Cette dernière doit alors arrêter de traiter les données concernées.

En vertu des dispositions juridiques de l'article 23 de la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

13-YOUNES-FELLOUS Vanessa, CASTETS-RENARD Céline, CHERUY Laurent, BLUM Patrick, BEAUGRAND Thomas, *Protection des données personnelles*, 2ème éd., Législatives, 2019, p. 68.

Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.

Le responsable du traitement, lorsque le traitement est effectué pour son compte, doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et il doit veiller au respect de ces mesures.

Il est interdit de transférer des données vers un Etat étranger sauf si ce dernier assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes.

II- La protection juridique plus efficace des données personnelles face aux droits des salariés

Il convient de noter qu'au Maroc les règles juridiques ne parviennent pas suffisamment à réglementer le domaine informatique surtout pénalement. Il est nécessaire donc de créer un cadre juridique plus compatible aux enjeux de l'époque numérique, puis veiller à son application à travers des mécanismes juridiques et institutionnels (CNDP et le pouvoir judiciaire) garantissant une mise en œuvre efficace en vue d'atteindre les objectifs escomptés par le législateur marocain, que ce soit sur le plan juridique ou économique.

A- Les insuffisances juridiques relatives à la protection des données personnelles des salariés

A la lecture et l'analyse juridique de la législation en vigueur il est à constater un ensemble de lacunes juridiques qu'il est nécessaire de revoir.

1- Difficulté de maîtrise des données personnelles des salariés

Le principe de recueil du consentement des salariés fait quant à lui l'objet d'un scepticisme croissant[14].

Il est judicieux de mettre en place un régime spécial pour l'hébergement de ces données, par exemple les données de santé des salariés présentant des caractéristiques qui justifient des mesures de protection spécifiques.

14- DESGENS-PASANAU Guillaume, op. cit., p. 62.

Les hébergeurs devraient être titulaires d'un agrément du ministre de la santé.

La législation devrait prévoir des dispositions juridiques qui sanctionneraient d'un emprisonnement de 3 ans d'emprisonnement et d'une forte amende le fait de proposer une prestation d'hébergement de données de santé, sans être titulaire de l'agrément.

Ainsi la question de traçabilité des données prises sans consentement du salarié concerné, ni d'une autorisation préalable par CNDP au Maroc, pose la problématique de la responsabilité en cas d'éventuel préjudice subi.

Toutefois, depuis l'adoption de la loi n°09-08 en 2009, plusieurs évolutions ont eu lieu à l'échelle internationale concernant la protection des données personnelles notamment, l'adoption par la commission européenne d'un nouveau règlement sur la protection des données à caractère personnelle (RGPD). Il s'agit du plus grand changement aux règles européennes relatives à la protection des données opéré au cours de ces vingt dernières années et plus[15]. Pour ce faire, il instaure un cadre uniforme pour la législation en matière de protection des données dans l'ensemble de l'Union Européenne.

2- Des mesures juridiques incompatibles, inadaptées et imprécises

Le traitement automatisé des données personnelles des salariés rend plus difficile la découverte et la détection des infractions en la matière et ça revient à l'absence d'une traçabilité matérielle d'une telle infraction et l'aspect parfois extraterritorial de ces infractions accentue de plus le problème lié à leur découverte[16].

Il convient de noter que la preuve des infractions constitue aussi l'une des insuffisances entachant la protection efficace des données à caractère personnel puisque en cas d'un traitement automatisé on assiste souvent à l'absence d'un élément matériel sur lequel le salarié peut se baser pour prouver l'infraction.

De même les procès-verbaux de la police judiciaire comme moyen de preuve prévu par la loi n°09-08 demeure incompatible avec un tel genre d'infraction nécessitant des procédés et moyens techniques spécifiques, à cela s'ajoute la faible force probante des procès-verbaux dressés par les agents de la CNDP, ce

15- HASS Gérard, *Guide Juridique du RGPD*, 2eme éd., ENI, 2020, p. 32.
16- LE GUYADER Patrick, op. cit., p. 47.

qui entrave une meilleure protection des données à caractère personnel des salariés[17].

Mais ces sanctions restent toujours insuffisantes et plus au moins légères lorsqu'on arrive à comprendre que les droits et la vie privée des salariés sont en question. Surtout à l'encontre des personnes morales responsables du traitement, de telles sanctions pénales ne semblent pas assez dissuasives et nécessitent d'être un peu plus sévères.

B- Pour une meilleure protection des données personnelles des salariés

Un usage contrôlé et systématisé de données personnelles des salariés ainsi qu'une réglementation plus claire et efficace des responsabilités correspondantes permettraient d'accroître davantage la qualité du traitement de données et faciliterait le contrôle des processus correspondants.

1- Renforcement des mesures juridiques des données personnelles des salariés

L'employeur, en sa qualité de responsable de traitement, doit porter à la connaissance des salariés de cet acte se rapportant sur leurs données personnelles.

Ainsi, le contrat de travail, devrait être le support le plus adapté pour donner une telle information et reprendre par exemple certaines dispositions de la politique de confidentialité de l'entreprise.

Il convient de noter que la législation devrait prévoir la possibilité d'ajouter une clause sur la protection des données personnelles dans le contrat de travail qui renvoie à la politique de confidentialité.

L'entreprise devrait garder la preuve que le salarié a pris connaissance de la politique de confidentialité (par exemple envoi de ladite politique par e-mail avec accusé de réception, remise en main propre contre décharge, etc.) sans forcément devoir le mentionner dans le contrat de travail[18].

Force est donc de constater que la règlementation en matière de protection des données a impacté le droit du travail et le code du travail devrait être aménagé et

---

17- BANCK Aurélie, BENSOUSSAN-BRULE Virginie, COQUER Anthony, ENTRAYGUES Dominique, *Le data protection officer*, 2eme éd., Bruylant, 2018, p. 79.
18- BANCK Aurélie, op. cit., p. 32.

s'avère une nécessité pour qu'il soit en diapason avec la législation relative à la protection des données personnelles.

Il convient de noter que la législation devrait prévoir des nouvelles obligations, qui s'ajoutent à celles déjà prévues dans loi n°09-08 de 2009, portant notamment sur la protection des données des salariés et à l'information de ces derniers sur les traitements effectués dans l'entreprise.

Afin de garantir aux salariés le respect de leurs droits, la législation devrait leur offrir des possibilités de recours accrues et d'étoffer l'arsenal de sanctions qui peuvent être prononcées par la CNDP.

La législation devrait prévoir davantage de droits en faveur des salariés sur leurs données personnelles :

- La **durée de conservation des données** ;
- L'existence des **droits de portabilité des données, de limitation du traitement ou d'effacement des données, ou de retrait de leurs consentements** ;
- **Le droit d'introduire une réclamation auprès de la CNDP.**

Il est également judicieux d'envisager des dispositions juridiques interdisant à l'employeur d'installer des caméras dans ses locaux sans définir un objectif, qui doit être légal et légitime. Par exemple, des caméras peuvent être installées sur un lieu de travail à des fins de sécurité des biens et des personnes, à titre dissuasif ou pour identifier les auteurs de vols, de dégradations ou d'agressions.

2- Durcissement des sanctions encourues en cas de violation de la législation

D'après l'article 30 de la loi n°09-08, ladite commission peut, quand bien même, contraindre les responsables de traitement des données personnelles à respecter leurs obligations vis-à-vis de la législation sous peine de sanctions de minime importance.

De ce fait, le deuxième paragraphe énonce la possibilité pour la commission d'ordonner que lui soit communiqué, dans les délais et selon les modalités ou sanctions éventuelles qu'elle fixe, les documents de toute nature ou sur tous supports lui permettant d'examiner les faits concernant les plaintes dont elle est

saisie. Toutefois, il est nécessaire que la loi n°09-08 et son décret d'application déterminent la nature et la consistance de telles sanctions.

Or, dans le cas où le responsable de traitement de données personnelles aurait refusé de s'exécuter, la loi devrait prévoir des sanctions qui lui seront infligées. Il reste que ce refus sera mentionné sur un procès-verbal qui sera transmis au procureur du Roi pour l'ouverture d'une information pénale.

La législation devrait prévoir des sanctions administratives pour les contrevenants tels que les avertissements, les blâmes, le retrait des autorisations ainsi que la publication des noms des organismes sanctionnés.

Tous les dossiers traités par la CNDP devraient être transmis au procureur pour des sanctions pénales. En fait, l'information du procureur du Roi par les agents commissionnés de la CNDP de toute opération de contrôle[19] dans un délai de vingt-quatre heures avant la date de ladite opération constitue également un obstacle à la célérité de la procédure de contrôle sur place. Enfin, aucune saisie de matériels objets de l'infraction ne pourrait être faite par les agents de la commission que sur l'autorisation du procureur du Roi compètent. Il est nécessaire d'envisager des sanctions administratives prononcées contre l'employeur en cas de manquement aux obligations à édicter par la législation.

Outre les différents recours que pourrait être menés par les salariés, la CNDP pourrait être habilitée à prononcer des mesures correctrices à l'encontre des entreprises ayant commis un manquement aux obligations dont notamment :

- Prononcer un avertissement ;
- Mettre en demeure l'entreprise ;
- Limiter temporairement ou définitivement un traitement ;
- Suspendre les flux de données ;
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- Ordonner la rectification, la limitation ou l'effacement des données.

Selon l'infraction constatée, des amendes administratives particulièrement lourdes pourraient être également prononcées. Leur montant peut ainsi aller jusqu'à 20 millions de dirhams, ou de 5 à 10% de son chiffre d'affaires annuel.

19- Article 19 du décret d'application de la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Quant au pouvoir judiciaire, son rôle à jouer en la matière est très déterminant mais dans le cas du Maroc le manque d'expérience et de formation des ressources humaines dans le domaine informatique et numérique constitue un obstacle devant une protection efficace des données à caractère personnel[20]. Donc, il est nécessaire d'opter pour un travail bien concerté dans ce sens en faisant participer plusieurs intervenants.

Conclusion :

En guise de conclusion, dans un essai ambitieux de garantir la protection juridique des données personnelles des salariés, le Maroc s'est doté au cours des deux dernières décennies d'un arsenal juridique spécifique au traitement des données à caractère personnel à travers l'avènement de la loi n°09-08 et ses textes d'application. Un arsenal juridique instituant au même temps un dispositif institutionnel sous le nom de la CNDP pour contrôler, réguler et surtout renforcer la protection des données à caractère personnel. Un droit jeune révélatrice de plusieurs indices permettant de l'évaluer en terme d'efficacité concernant la protection des données à caractère personnel et la garantie des droits et libertés individuels face au traitement des données personnelles dans le milieu du travail[21]. En plus des insuffisances juridiques constatées en matière de protection des données à caractère personnel, le dispositif institutionnel dont dispose le Maroc, la CNDP et le pouvoir judiciaire, ne lui permet pas de garantir une protection assez efficace en la matière.

20- DESGENS-PASANAU Guillaume, op. cit., p. 67.
21- BENSOUSSAN Alain, op. cit., p. 82.

Bibliographie :

- **Ouvrages :**

- BENSOUSSAN Alain, *La protection des données personnelles de A à Z*, 1re éd., Bruylant, 2017.
- BANCK Aurélie, *RGPD : la protection des données à caractère personnel*, 3éme éd., Gualino, 2018.
- BANCK Aurélie, BENSOUSSAN-BRULE Virginie, COQUER Anthony, ENTRAYGUES Dominique, *Le data protection officer*, 2eme éd., Bruylant, 2018.
- DESGENS-PASANAU Guillaume, *La protection des données à caractère personnel*, éd., Lexis Nexis, 2018.
- HASS Gérard, *Guide Juridique du RGPD*, 2eme éd., ENI, 2020.
- LAFFAIRE Marie-Laure, *Protection des données à caractère personnel tout sur la nouvelle loi*, éd., Eyrolles, 2005.
- METILLE Sylvain, *Protection des données*, éd., Helbing Lichtenhahn Verlag, 2019.
- LE GUYADER Patrick, *Protection des données sur internet*, éd., Lavoisier, 2013.
- YOUNES-FELLOUS Vanessa, CASTETS-RENARD Céline, CHERUY Laurent, BLUM Patrick, BEAUGRAND Thomas, *Protection des données personnelles*, 2ème éd., Législatives, 2019.

- **Articles :**
- BENSOUSSAN Alain, « Internet : aspects juridiques », in Petites Affiches, n°134, 1996.
- MARTIN Daniel, « La criminalité informatique », in P.U.F., 1997.

- **Textes juridiques :**
- Loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.
- Décret n°2-09-165 du 21 mai 2009 pris pour l'application de la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.
- Décision du premier ministre n°3-33-11 du 28 mars 2011 approuvant le règlement intérieur de la Commission nationale de contrôle de la protection des données à caractère personnel, Bulletin Officiel n°5932 du 7 avril 2011.
- Directive européenne n°95/46/CE.

الجلسة العلمية الثانية

رئيس الجلسة

الدكتور محمد مومن

أستاذ التعليم العالي، كلية العلوم القانونية والاقتصادية والاجتماعية - جامعة القاضي عياض مراكش.

إستراتيجيات الأمن السيبراني في التشريعات العربية ﴿اليمن أنموذجا﴾

الدكتور محمد علي محمد قيس
نائب رئيس جامعة سبأ للشؤون الأكاديمية،
وعميد كلية الحقوق (اليمن)
dr.gess2014@gmail.com

الملخص:

الأمـن عنصر ضروري في الحيـاة وركيزة أساسية لبناء أي مجتمع ونمو نشاطه؛ ومع بروز الثورة التكنولوجية تعاظم دور تكنولوجيا المعلومات والاتصالات، وبتزايد أثرها على مؤسسات الدولة، ازدادت المخاطر على المنظومات المعلوماتية، وتنوعت واختلفت أساليبها، مما أدى إلى تعطيل الخدمات العامة، وإيقاع خسائر مادية ومعنوية بالأفراد والمؤسسات الحكومية، وعرف ما يسمى بالحرب الإلكترونية، وهنا برز مصطلح الأمن السيبراني(Cyber security) ، فتعتبر قضية الأمن السيبراني من أهم القضايا التي تشغل العالم اليوم؛ لأنه جزء أساسي مـن أمـن الدولـة لرتبا طه بالمسائل المتعلقة بحمايـة المعلومـات لما لها من تأثير فعال لأمن القومي والاستقرار الاقتصادي. ومع الإقرار بخطورة التهديد السيبراني، بحث خبراء الأمن، وصناع القرار، والمشرعين استراتيجية التصدي للهجمات السيبرانية، فبدون الردع السيبراني ستظل البيانات المفتوحة عرضة للاختراقات والاعتداء والاستغلال.

الكلمـات المفتاحيـة: الأمـن – السيبراني – الإستراتيجية – التشريعات.

Résumé:

Security is a necessary element in life and a fundamental pillar for building any society and growth of its activity. With the emergence of the technological revolution, the role of information and communication technology increased, and its impact on state institutions increased, also the risks of information systems increased, and their methods varied, which led to the disruption of public services, and the infliction of material and moral losses on individuals and governmental institutions, and the so-called electronic war, and here the term emerged Cyber security. The issue of cyber security is one of the most important issues that occupy the world today. Because it is an essential part of state security and it is linked to issues related

to the protection of information and its effective impact on national security and economic stability. While recognizing the seriousness of the cyber threat, security decision makers and lawmakers discussed a strategy to respond to cyber-attacks. Without cyber deterrence open data will remain vulnerable to breaches, abuse, and exploitation.

Keywords: security - cyber security - strategy - legislation.

المقدمة:

في ظل الثورة الرقمية المعاصرة، والتطور الهائل في وسائل الاتصال وأجهزة الاتصالات في كل مناحي الحياة، أصبحت تكنولوجيا المعلومات والاتصالات المحرك الأساسي في عملية جمع المعلومات وتبادلها وحفظها ومعالجتها، الأمر الذي يساهم في نمو مختلف القطاعات الاقتصادية والاجتماعية، وحيث أن شبكة الإنترنت تعتبر مخزن كبير للمعلومات، والأدوات الأساسية في التفاعلات المختلفة بين الأفراد والمؤسسات، ومنصة للتطبيقات التعليمية والعلمية وتقديم خدمات الكترونية لجميع مؤسسات المجتمع الرسمية منها والتجارية، مما جعل العالم الالكتروني والفضاء السيبراني ساحة للصراعات الدولية سواء كانت مدنية أو عسكرية، حيث أن قوة الدول لم تعد تقليدية اقتصاديًا وعسكريًا فقط، وإنما برز ما يعرف بالفضاء السيبراني، واصبح من يمتلك التكنولوجيا هو من يملك القوة والسيطرة، وبرزت مخاطر عسكرة الفضاء الإلكتروني، فتسعى الأنظمة والدول جاهدة لحماية فضائها الإلكتروني وتأمين بياناتها.

وعلى الرغم من التطور الهائل الذي شهدته اليمن في مجال الاتصالات وتقنية المعلومات وإدخال خدمة الانترنت منذ عام 1996م، ومع توجه الحكومية نحو الأتمتة، أصبح الحفاظ على استمرارية الاتصال وسهولة وسرعة الوصول إلى شبكة الإنترنت أمرا حيويا وأساسيًا لا غنى عنه، وبالتالي ستتزايد المخاطر والاختراقات والتهديدات السيبرانية على السيادة الوطنية والأمن القومي، ولهذا فإن بناء ثقافة الأمن السيبراني بات أمرًا أساسيًا. (1)

إن الأوضاع الأمنية غير المستقرة التي تشهدها اليمن، تحتاج إلى الأمن السيبراني؛ لأن مجال المعلومات في اليمن لم يحظَ بالاهتمام من مختلف القطاعات سواء كانت حكومية أو خاصة، مع أن خبراء أمن المعلومات قد كشفوا أن اليمن تعتبر أرض خصبة للإرهاب الالكتروني. (2)

وبناء على ما سبق ومع الإقرار بخطورة التهديدات السيبرانية تبحث الحكومة اليمنية، مع الخبراء والباحثين بضرورة تأمين بنية تحتية آمنة لتقديم الخدمات الإلكترونية، وكشف محاولات الاختراق واتخاذ الإجراءات اللازمة بأسرع وقت ممكن في حال حدوثها، فقد أعدت وزارة الاتصالات وتقنية المعلومات سياسة وطنية لأمن المعلومات؛ والتي تتضمن المتطلبات الأساسية الواجب توفرها لدى الجهات الحكومية لضمان عمل المنظومات المعلوماتية بشكل آمن ومستمر، وبعد أن شعرت الوزارة بمخاطر غيات منظومة لأمن المعلومات، دعت إلى عقد مؤتمر خاص لتوعية القطعات المختلفة في الدولة لحماية المعلومات.

أهمية وهدف الدراسة:

هذه ورقة متواضعة نظرية تهدف إلى إلقاء ضوء على أهمية الأمن السيبراني والتعريف به، وكيفية تحقيق الامن السيبراني لحماية المواطنين والمستهلكين وأجهزة الدولة، في ظل تزايد انخراط اليمن في استخدام تقنيات الفضاء الإلكتروني، وما يتصل بها من تهديدات للأمن القومي، وتوضيح أهمية مواجهتها بقواعد قانونية ضمن التشريعات الحالية حتى يرى النور مشروع قانون مكافحة جرائم تقنية المعلومات القابع تحت قبة البرلمان.

اشكالية الدراسة:

الإشكالية تتمثل في أن التكنولوجيا تتطور بشكل يومي والقانون لا يتطور بنفس الوتيرة المتسارعة، فلابد من مواكبة المستجدات والتطورات بقوانين تنظمها وتحميها.

فرضية الدراسة:

انتقال الصراع الدولي إلى الفضاء السيبراني زاد من احتمال حدوث حروب سيبرانية مما يتطلب من الحكومة اليمنة زيادة الاهتمام بالتطور التكنولوجي، وحمايتها قانونيا لتحقيق أمن المعلومات والفضاء السبراني

أسباب اختيار الموضوع:

- الحاجة الماسة لمعرفة مفهوم الأمن السيبراني ودوره في تحقيق حماية المعلومات.
- نشر ثقافة الأمن السيبراني.
- توضيح ما يحققه الأمن السيبراني من استقرار لتكنولوجيا المعلومات بما يعود الفائدة للمجتمع.

خطة الورقة:

تتكون الورقة من مبحثين

المبحث الأول: نخصصه لمفهوم الأمن السيبراني.

المبحث الثاني: نفرده للتبعات القانونية للأمن السيبراني في التشريعات اليمنية.

المبحث الأول: مفهوم الأمن السيبراني

بادئ ذي بدء نسمع كثيرًا عن أمن المعلومات وحماية المعلومات والحماية القانونية أو التشريعية للمعلومات، ومنذ عام 2014م برز مصطلح الأمن السيبراني، فما مدلول أمن المعلومات والأمن السيبراني؟

على الرغم من أن الغالبية يظنون بأن الأمن السيبراني وأمن المعلومات أنهما مصطلحان مترادفان يقصد بهما حماية المعلومات، إلا أن الفقه يفرق بين مدلول المصطلحين فالأمن السيبراني يهتم بحماية المعلومات من التعرض للسرقة من قبل مصادر خارجية على شبكة الإنترنت، بينما أمن المعلومات يهتم بالمعلومات أينما وجدت. (3)

الامن السيبراني:

هو الأمن الذي يتعلق بالحماية من المخاطر المحتملة عن طريق مصادر خارجية وخاصة الإنترنت، وحماية الحواسيب المكتبية أو المحمولة من أي نوع من الهجمات والاختراقات والتهديدات التي تحدث عن طريق السيرفرات والحواسيب الأخرى وشبكة الإنترنت بشكل عام، وعدم السماح لأحد غير مصرح له بالدخول أو الوصول إلى المعلومات .(4)

أمن المعلومات:

يهتم أمن المعلومات بحماية كل ما يتعلق بالمعلومات ضمن الحاسب وليس حماية الحاسب كله، وتصنف البيانات على أنها معلومات عندما تكون ذات معنى، حيث أن كل ما يحفظ ضمن أي نظام حاسوبي يدعى بيانات ولكنها لا تسمى معلومات إلا حين تتم معالجتها لتأخذ معنى، أي تصبح صورة يمكن رؤيتها أو نص يمكن قراءته أو ملف ما يمكن تشغيله، وهنا يتدخل أمن المعلومات ويقوم بحمايتها من أي خطر خارجي محتمل كالسرقة والاختراق ويمنع أي شخص غير مصرح له بالوصول إليها

كثير من الباحثين يميلون إلى أن مصطلح سيبار ظهر مع ظهور الشبكة العنكبوتية الانترنت، إلا أن الأمن السيبراني ظهر حديثًا وعرف بأنه جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها الالكترونية والمادية من مختلف الجرائم، والهجمات أو هو عبارة عن مجموعة الوسائل التقنية والتنظيمية

والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به، وسوء الاستغلال، واستعادة المعلومات الإلكترونية، ونظم الاتصالات والمعلومات التي تحتويها، وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات، وتعزيز حماية وسرية وخصوصية البيانات الشخصية، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني. (5)

بقدر ما أعطت الحواسيب والإنترنت خدمات وتسهيلات ومعارف، أعطت في نفس الوقت عالم الجريمة أبعاد جديدة، فصار من الممكن ارتكاب جرائم السرقة، والتزوير، والاختلاس عن بعد، فظهر مصطلح (Cybercrime) الذي يعني الجرائم التي ترتكب باستخدام الحاسوب بواسطة شبكة الإنترنت.

فالفضاء السيبراني يتعلق بضبط الاتصالات، وانتقال المعلومات، ويتعلق بأمن المواقع والأنظمة الالكترونية، ولهذا فإن الأمن السيبراني حزمة من العمليات والإجراءات تقوم بحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجوم أو التلف أو السرقة والوصول غير المصرح به. (6)

المفهوم الفقهي للجريمة المعلوماتية:

الجريمة بصورة عامة هي سلوك إجرامي مضر بمصالح المجتمع من خلال ارتكاب فعل يجرمه القانون أو الامتناع عن فعل أمر به القانون، فإذا ما تم هذا الفعل بواسطة الوسائل التكنولوجية بواسطة الحاسوب وعبر شبكة الإنترنت يمكن وصف النشاط حينئذ بالجريمة الإلكترونية. عرفها جانب من الفقه بأنها كل فعل غير مشروع يؤدي فيه جهاز الحاسوب دورًا مهمًا لإتمام السلوك غير المشروع على أن يكون هذا الأداء أو الدور مؤدي إلى ارتكاب الجريمة. (7)

ومن الفقهاء من عرف الجريمة المعلوماتية بأنها: " كل أشكال السلوك أو الفعل غير المشروع والذي يرتكب بواسطة جهاز الحاسوب. (8)

وعرفها جانب آخر من الفقه بأن الجريمة المعلوماتية تشمل كل أشكال السلوك أو الأفعال التي تضر بالمجتمع والتي ترتك باستخدام الحاسب الآلي والإنترنت. (9)

مكتب تقييم التقنية الأمريكي بأنها: " مجموعة من الأفعال المرتبطة بالمعلومات التي يمكن أن تكون جديرة بالعقاب"(10)

خصوصية جرائم الإنترنت والحلول الفقهية المقترحة بشأن تنازع الاختصاص :(11)

كما هو معلوم، فإن الشبكة العنكبوتية لا تستأثر بها دولة بعينها، ويتسنى لمستخدميها ولوجها من أية بقعة في العالم تقريبًا من خلال جهاز حاسوب يكون متصلاً بها، وبما أن الشبكة موزعة على الكرة الأرضية، لا تتقيد بالحدود، تكون من حيث المبدأ خارج أية رقابة أو سيطرة من أية جهة، وهذا يستتبع ولو نظريًا ـ عدم إمكان خضوعها لسلطان قانون معين .(12)

صعوبة إثبات الجرائم المعلوماتية، يعود ذلك لصعوبة إقامة الدليل المادي على مرتكبها؛ لأن المجرم المعلوماتي يقوم بمحو الدليل، والتلاعب فيه، ويعود ذلك لطابعة التقني. (13)

القطاعات المستهدفة في مجال جرائم نظم المعلومات: (14)

إن كافة المجالات والأنشطة والقطاعات سواء الحكومية أو الخاصة، أمست تستخدم الحاسب الآلي والإنترنت، وتعتمد عليهما نظرًا للإمكانيات العالية والخدمات والتسهيلات التي تقدمه بالمقارنة بالجهود البشرية، بما أصبح يعرف بالحكومة الإلكترونية، التي تعتمد على حاسبات ترتبط بعضها ببعض بشبكة داخلية، وترتبط هذه الشبكة بالشبكة الدولية الإنترنت عن طريق وسائل الاتصالات الحديثة، ومن خلال هذه الشبكات تتداول بيانات ومعلومات الحكومة الإلكترونية، ولهذا فإن كافة المجالات والأنشطة والقطاعات، ليست بمنأى عن ظاهرة الجريمة الإلكترونية، ولهذا فإن الحاجة ملحة للأمن السيبراني. وقد نما إلى جوار السوق الشرعية للمعلومات السوق السوداء للمعلومات ذلك السوق الذي تتم فيه مقايضة وبيع المعلومات المسروقة أو المقتبسة من أصحابها الحقيقيين والشرعيين، وخاصة في الأنشطة الاقتصادية والاجتماعية والتي نالت المعلومات الأتية:(15)

- المعلومات المالية، سواء في المنشئات العامة والخاصة،
- المعلومات التجارية والصناعية، حيث تستهدف مشروعات الاستثمار، والتصنيع، والإنتاج، والأسواق، والتوزيع، ومراكز البيع، والأسعار، وقطاع الصناعي للإنتاج.
- المعلومات الشخصية، التي تمس سرية الحياة الخاصة، والنقابية، والسياسية، المخزنة في ذاكرة الحاسبات الآلية للنوك وشركات التأمين، وكذلك التي لدى المحامين، والمستشفيات، وفي الشرطة، والأحزاب، والنقابات.
- المعلومات العسكرية، التي تمس أسرار الدولة والمشروعات التسليحية المختلفة وخاصة الحديثة.

الجهود الدولية لمكافحة الجرائم المعلوماتية: (16)

الجهود الدولية لمكافحة الجرائم المعلوماتية، ما زالت دون المستوى المطلوب رغم بعض الجهود التي لا ترقَ إلى المستوى التعاون المطلوب. وعملاً بمبدأ الإقليمية، فإن كل دولة تمارس سيادتها على إقليمها بتطبيق قوانينها داخل حدودها، بصرف النظر عن جنسية مرتكب الجريمة، الذي يحتمل معه تنازع القوانين حيال الواقعة الواحدة، والذي يستتبع بالضرورة تنازع الاختصاص. فجريمة السب مثلاً عبر الرسائل الإلكترونية E. mails تقع أحياناً في بلد ويتلقاها الضحية في بلد آخر، فمثل هذه الرسائل وغيرها التي تتم عن بعد بواسطة هذه الشبكة تمر في كثير من الأحيان بأكثر من دولة قبل وصولها إلى بلد الاستقبال، ناهيك أن بعض الأفعال التي تبث من خلال الإنترنت، تعد أحياناً جريمة في بلد ومباحة في غيره من البلدان المرتبطة بهذه الشبكة . مما يزيد من انعدام أو ضعف الرقابة على الرسائل الإلكترونية، وغياب قانون محدد يجري إعماله على الأفعال التي تكون جرائم انترنت، مما يثير التساؤل عن القانون الواجب التطبيق على المواقع الإلكترونية على شبكة الإنترنت .

وتطبيقاً للقواعد التي تحكم الاختصاص المكاني، فإن جرائم الإنترنت العابرة للحدود تخضع في كثير من الأحيان لأكثر من قانون، فإذا وقع السلوك في نطاق بلد معين والآثار الضارة تحققت في نطاق بلد آخر، فإن كلا البلدين يكون قانونه واجب التطبيق على الواقعة، بمعنى أنه يتم تطبيق قانون كل دولة تحقق في نطاقها أحد عناصر الركن المادي للجريمة (السلوك أو النتيجة)، فيكفي ليكون قانون البلد واجب التطبيق تلقي الضحية الرسالة الإلكترونية المجسدة لجريمة السب أو التهديد مثلاً في نطاقه ولو كان الفعل ذاته غير معاقب عليه في بلد المنشأ . وبتطبيق ذلك على جريمة انتهاك المصنفات ينعقد الاختصاص للدولة التي تم فعل الانتهاك على إقليمها، باعتبار أن الفعل عن بعد يعد أحد العناصر المكونة لجريمة التقليد، وثمة أمر آخر يزيد الأمر تعقيداً وصعوبة في تحديد الاختصاص في جرائم الإنترنت عبر الوطنية بالذات ألا وهو تباين المعايير الوطنية فيما يتعلق بتحديد الاختصاص، الأمر الذي يفضي عادة إلى حدوث تنازع في الاختصاص بشأن هذه الطائفة من الجرائم .

فعلى سبيل المثال، لو أن شخصاً ارتكب أياً من هذه الجرائم على إقليم دولة لا يحمل جنسيتها، فقد يحدث التنازع بين قانون الدولة التي ارتكبت الجريمة على إقليمها وقانون الدولة التي ينتمي إليها، أي أن الفعل يتنازعه قانونان، قانون دولة الإقليم على أساس مبدأ الإقليمية، وقانون دولة الجاني على أساس مبدأ الشخصية.

وعلى افتراض إمكانية إيجاد حل لهذه المشكلة من الناحية القانونية، فإنها تظل تصطدم بعقبات عملية بالنظر إلى الإجراءات المعقدة والطويلة التي يلزم اتباعها لمحاكمة الجاني الذي ارتكب أيًا من هذه الجرائم، المقيم خارج البلد الذي تتم فيها محاكمته، وعلى تنفيذ الأحكام الصادرة بالخارج، خاصة أن العائق الأكبر مبدأ عدم جواز محاكمة الشخص عن الفعل الواحد مرتين، وكذلك عدم جواز تسليم الوطنيين .

وقد طُرحت مثل هذه المشاكل على القانون المقارن، فالقانون الأمريكي يتسع نطاق تطبيقه بحيث يمتد إلى الأفعال المرتكبة في الخارج طالما أن آثارها تحققت في الولايات المتحدة الأمريكية، وتشير التطبيقات القضائية إلى أنه يكفي لامتداد ولاية القضاء المذكور إلى جريمة وقعت في الخارج أن تكون آثارها قد مست مصالح أمريكية أو عرضتها للخطر، وفقًا لمبدأ الاختصاص الشخصي.

كما تبنى القضاء الإنجليزي نظر الدعاوى الناشئة عن إساءة استخدام الإنترنت، متى كان هناك ارتباط بين الواقعة المرتكبة وبريطانيا عملاً بقانون إساءة استخدام الحاسوب الصادر سنة 1990م (The Computer Misuse Act of 1990، فلكي ينعقد الاختصاص للمحاكم الإنجليزية، يكفي امتداد آثار الواقعة إلى بريطانيا، ولو كانت هذه الواقعة قد حدثت في الخارج، بصرف النظر عن محل إقامة. أما في فرنسا فيمتد اختصاص القضاء هناك إلى جرائم الإنترنت التي وقعت في الخارج عملاً بقانون العقوبات الجديد متى كانت الظروف الواقعة تبرر مصلحة فرنسا في إعمال قانونها عليها .

نخلص مما سبق إلى إن جرائم الإنترنت عبر الوطنية، لا تتقيد بحدود خلافًا للجرائم التقليدية المعروفة، الأمر الذي يجعلها في كثير من الأحيان تستعصي الخضوع للقواعد القانونية التي تحكم مسألة الاختصاص المكاني، ومن ثم فإن الطبيعة الخاصة لهذا الصنف من الجرائم العصرية تتطلب تجاوز المعايير التي طرحها الفقه للتغلب على مشكلة تنازع الاختصاص والعمل على تبني حلول أكثر مرونة تأخذ في الحسبان النطاق الجغرافي لهذه الجرائم وسهولة ارتكابها وآلية تنفذها والتخلص من آثارها وما إلى ذلك من اعتبارات يفرضها الطابع التقني المتطور.

ولهذا ينبغي ألا يترك الأمر لمحض اجتهادات الفقه والقضاء، وإنما يلزم تدخل المشرع لتحديد معايير الاختصاص التي يفترض عدم تضييق نطاقها، بحيث يكون من الملائم أن ينعقد الاختصاص لقانون أي بلد أضرت به الجريمة أو المتوقع أن تشكل خطورة على مصالحه، ولو كان مكان وقوعها خارج نطاق إقليمها وفي تقديرنا فإن تبني مبدأ الاختصاص العالمي بهذا الخصوص من أجل تجنب الكثير من المشاكل الناجمة عن تحديد مكان وقوع الجريمة أو ترتب آثارها الضارة.

المبحث الثاني: التبعات القانونية للأمن السيبراني في التشريعات اليمنية

لقد أصبحت البرامج وتطبيقاتها، وقواعد البيانات، تلعب دورًا كبيرًا في نظم الحاسوب الآلي، وتؤثر تأثيرًا مباشرًا في نجاح استخداماتها المختلفة، فمن الضروري أن يتدخل المشرع لحمايتها، سيما وأن المصنفات التقليدية في الوقت الحالي مثل الكتب والمجلات قابلة للنسخ في شكل الكتروني. (17)

موقف التشريعات العربية من الجريمة المعلوماتية:

الملاحظ أن جميع دول العالم تسعى نحو تأمين أنظمتها المعلوماتية ومنها الدول العربية، وإن كانت الأخيرة تسير في سبيل الوصول إلى منظومة تأمينية لأنشطتها المعلوماتية بخطى بطيئة نسبيًا؛ لأنها كانت تعتمد إلى حد كبير على القواعد الجنائية لمواجهة ظاهرة الجريمة المعلوماتية وذلك بمحاولة تطويع النصوص العقابية القائمة للتطبيق على الأفعال المختلفة للجريمة المعلوماتية، فهذا هو الحال اليمني فلم يصدر بها قانون خاص بالجريمة المعلوماتية.

الإسكوا والتشريعات السيبرانية في المنطقة العربية: (18)

لجنة الأمم المتحدة الاقتصادية والاجتماعية لغرب آسيا (United Nations Economic and Social Commission for Western Asia) وتعرف باسم إسكوا (ESCWA) وهي واحدة من خمس لجان إقليمية أسسها المجلس الاقتصادي والاجتماعي للأمم المتحدة ومقرها الرئيسي في بيروت، لبنان. في 9 آب/أغسطس 1973م تأسست الإسكوا بموجب قرار المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة 1818 (LV) (د-55) لتحل محل مكتب الأمم المتحدة الاقتصادي والاجتماعي في بيروت، وقد تبدل الاسم عام 1985م، سميت آنذاك "اللجنة الاقتصادية لغربي آسيا (الإسكوا).

- 26تموز/يوليو 1985م أعيدت تسميتها فأصبحت "اللجنة الاقتصادية والاجتماعية لغربي آسيا" (الإسكوا)، وذلك بهدف الإقرار بالجانب الاجتماعي من عملها.
- 1982-1991م انتقلت الإسكوا من بيروت إلى بغداد إثر الاجتياح الإسرائيلي للبنان في عام 1982م، وبقيت في العاصمة العراقية حتى عام 1991م.
- 1991-1997م انتقلت الإسكوا من بغداد إلى عمّان إثر حرب الخليج الثانية في عام 1991م، وبقيت في العاصمة الأردنية حتى عام 1997م.
- تشرين الأول/أكتوبر 1997م عادت إلى بيروت، العاصمة اللبنانية، التي كانت المقر الدائم لها.

لقد أظهرت الدراسات التي أجرتها الإسكوا أن معظم البلدان العربية تعاني من الفراغ التشريعي في المواضيع الخاصة بالفضاء السيبراني، يعود ذلك بشكل أساسي إلى حداثة هذه المواضيع، وارتباطها بالتطورات السريعة لتكنولوجيا المعلومات والاتصالات، يضاف إلى ذلك بطء عملية صياغة وإقرار القوانين في معظم البلدان العربية، نتيجة لعدم الاستقرار السياسي في المنطقة؛ كما أن تقاطع التشريعات السيبرانية مع العديد من القوانين القائمة يشكل صعوبة إضافية أمام البلدان، لا سيما القوانين المتعلقة بتنظيم قطاع الاتصالات، والقوانين الجنائية، إذ إن إدخال بنود خاصة بالجريمة الإلكترونية أو إصدار قانون خاص بذلك يتطلب جهود كبيرة من أجل تحديد ماهية الجرائم الإلكترونية وكيفية إثباتها وعقوباتها، بما يتلاءم مع الإطار الفقهي والقانوني للبلد،.(19)

وإزاء تكرار توصيات المشاركين في اجتماعات الإسكوا على ضرورة القيام بعمل إقليمي يسعى إلى تنسيق القوانين على مستوى البلدان العربية يستجيب للحاجة والنقص فيها، قامت الإسكوا بإطلاق مشروع "تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية" الذي بدأ تنفيذه عام 2006م وانتهى بنهاية عام2012م وقد هدف هذا المشروع إلى تعزيز وتنسيق التشريعات السيبرانية في المنطقة العربية بغية بناء قطاع متين ومستدام لتكنولوجيا المعلومات والاتصالات عبر وضع الأطر التشريعية والقانونية الملائمة، وقد حاول بعض البلدان العربية استدراك هذا الفراغ التشريعي عبر سن قوانين تتعلق بالمعاملات الإلكترونية وذلك باقتباس قواعد قانونية من بلدان أخرى أو بالاستعانة بالمعاهدات الدولية، إقرارًا منها بأهمية هذه التشريعات وضرورتها من أجل تطوير مجتمع المعلومات وبناء الاقتصاد المبني على المعرفة.(20)

والأمر لا يزال يحتاج لجهود مضنية لرفع أمن المعلومات في البلدان العربية، ولهذا تهتم القطاعات العامة والخاصة وخاصة الأكاديمية منها لعقدت ندوات ومؤتمرات عدة حول المتطلبات القانونية والتنظيمية لبناء مجتمع المعرفة المستدام في المنطقة العربية تم خلالها استعراض ومناقشة مقترح إطار عمل إقليمي للتشريعات السيبرانية في المنطقة العربية، والذي يحدد دور البلدان في تطوير التشريعات السيبرانية وطنيًا، ففي لبنان عدت ندوة في مقر الأمم المتحدة في بيروت يومي 19و20 كانون الأول/ديسمبر 2012م،(21) وفي اليمن عقد المؤتمر الوطني الأول للأمن السيبراني بمقر وزارة المواصلات وتقنية المعلومات بصنعاء في الأيام 7-9 من يونيو/حزيران 2021م.(22) وفي المملكة المغربية نظم المركز الدولي للخبرة الاستشاري، وماستر العلوم الجنائية والأمنية، كلية العلوم القانونية والاقتصادية والاجتماعية جامعة القاضي عياض، بمراكش، ومختبر بحث قانون الأعمال، كلية العلوم القانونية والسياسية جامعة الحسن الأول بسطات، ومجلة القانون والأعمال الدولية، عقد

المؤتمر العلمي الدولي تحت عنوان " لأمن السيبراني في التشريعات العربية"، المنعقد عن بعد يومي 16و17 يوليو/تموز2021م، ولقد تخلل تلك اللقاءات عروض ونقاشات حول التوجهات المستقبلية الوطنية والإقليمية والدولية، وتحديات التكنولوجيات الجديدة بالاهتمام بالأمن السيبراني وحماية مصنفات الحاسوب الآلي، ويمكن تصنيف التشريعات السيبرانية الموصى بها، تبعًا لموضوعها، في أربعة أنواع: (23)

- النوع الأول يتضمن القوانين الهادفة إلى حماية المستخدم مثل حماية الخصوصية والبيانات الشخصية وحماية حقوق المستهلك.
- والنوع الثاني يتعلق بالقانون الجزائية وهو خاص بمعالجة الجرائم والاستخدام السيء للفضاء السيبراني.
- النوع الثالث مرتبط بحماية الملكية الفكرية للمنتجات والبرامج والمعلومات المنشورة على الإنترنت بما يتلاءم مع تحفيز الإبداع ولابتكار.
- النوع الرابع يهدف إلى تنظيم الأعمال التجارية على الفضاء السيبراني.

موقف التشريعات اليمنية من أمن المعلومات:

كما سبق القول بأن لا يوجد قانون خاص يعالج الجريمة المعلوماتية، وبالتالي في القواعد التقليدية هي الحل، باستقراء القواعد القانونية نجد أنواع من القواعد القانونية التي تتعلق بالجريمة المعلوماتية، كالقواعد لتي تحمي حرمة الحياة الخاصة، وجرائم الأموال، والقواعد الواردة في تشريعات خاصة، والتي يمكن تطبيقها على الجرائم المعلوماتية، كالقوانين الخاصة بنظام الدفع الإلكتروني، وقانون الحق الفكري، تنظيم الصناعة، وقانون العلامات التجارية، وتصاميم الصناعية، وبراءة الاختراع، وحق المؤلف.

فالمشرع بالقطر العربي اليمني يعترف بالتعاقد بأي وسيلة اتصال طالما كانت مقبولة من الناحية القانونية، حيث نصت المـادة 154 مدني بقولها: " يتم العقد بواسطة كل وسائل الاتصالات السلكية واللاسلكية طالما توفرت فيها الصفة الوثائقية المقبولة قانونًا".(24)

والقانون رقم 40 لسنة 2006م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية عرف المصطلحات المتعلقة بالحاسبات على النحو الآتي: (25)

نظام معالجة المعلومات:	**المنظومة الإلكترونية المستخدمة لإنشاء رسائل البيانات ومعالجتها وتجهيزهـا وتخزينها وإرسالها واستقبالها.**
رسالة البيانات:	مجموعة من الأوامر والأرقام التي تحتاج إلى معالجة وتنظيم أو إعادة تنظيم لكي تتحول إلى معلومات، وقد تأخذ شكل نص أو أرقام أو أشكال أو رسومات أو صور أو تسجيل أو أي مزيج من هذه العناصر.
رسالة المعلومات:	هي عبارة عن بيانات تمت معالجتها بواسطة نظام معالجة المعلومات فأخذت شكلاً مفهومًا.
تبادل البيانات الإلكترونية:	نقل البيانات إلكترونياً من شخص إلى آخر باستخدام نظام معالجة المعلومات.
العقد الإلكتروني:	الاتفاق الذي يتم إبرامه بوسائل إلكترونية كلياً أو جزئيًا.
التوقيع الإلكتروني:	عبارة عن جزء مشفر في رسالة البيانات أو مضاف إليها أو مرتبط بها ويتخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون مدرجًا بشكل إلكتروني أو رقمي أو ضوئي أو أي وسيلة أخرى مماثلة بحيث يمكن من خلاله التعرف على المنشئ وتمييزه وتحديد هويته والتأكيد على موافقته على محتواها.

ونصت المادة الرابعة من هذا القانون على ما يأتي: يسري هذا القانون - وبما لا يتعارض مع أحكام قانون الاتصالات السلكية واللاسلكية- على جميع المعاملات التي تتناولها أحكامه وعلى وجه الخصوص ما يلي: -

1. أنظمة الدفع الإلكترونية، وسائر العمليات المالية والمصرفية التي تنفذ بوسائل إلكترونية.
2. رسائل البيانات والمعلومات الإلكترونية وتبادلها، والسجلات الإلكترونية.
3. التوقيع الإلكتروني، والترميز والتوثيق الإلكتروني.
4. المعاملات التي يتفق أطرافها صراحةً أوضمناً على تنفيذها بوسائل إلكترونية ما لم يرد فيه نص صريح يقضي بغير ذلك.

ونصت المادة العاشرة منه أيضًا على ما يأتي: " يكون للسجل الإلكتروني والعقد الإلكتروني ورسالة البيانات والمعلومات الإلكترونية والتوقيع الإلكتروني نفس لآثار القانونية المترتبة على الوثائق والمستندات والتوقيعات الخطية من حيث إلزامها لأطرافها أو حجيته في الإثبات".

ومن هذا المنطلق تعتبر رسالة المعلومات وسيلة من وسائل التعبير عن الإرادة المقبولة قانونًا لإبداء الإيجاب أو القبول بقصد إنشاء التزام تعاقدي.

وحيث أن المعلومات حق من حقوق الإنسان الأساسية في زمن المعلومات، حرص المشرع على ذلك واكد على ذلك بتشريع خاص سمي قانون حق الحصول على المعلومات نصت المادة الرابعة منه بقولها: "لحصول على المعلومات حق من حقوق الموطنين اليمنين الأساسية، بل وللأجانب المقيمين بالجمهورية اليمنية الحق الحصول على المعلومات شريطة المعاملة بالمثل". (26)

إن تنوع الجرائم المعلوماتية، سواء من حيث أساليب ارتكابها، والوسائل اللازمة لارتكابها أو من حيث الزمن الوجيز الذي قد يستغرق في ارتكابها، فبعض الجرائم قد يتم ارتكابها في زمن يعادل الضغط على أحد مفاتيح الحاسب الآلي، وهذا يتطلب تدخل القوانين للحد من الجريمة المعلوماتية، نصت المادة 41 من قانون أنظمة الدفع على أن : " يعاقب كل من يرتكب فعلاً يشكل جريمةً بموجب أحكام القوانين النافذة بواسطة استخدام الوسائل الإلكترونية بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن ثلاثمائة ألف ريال ولا تزيد على مليون ريال" .

ولا تقف القواعد القانونية التي يتضمنها نظام الملكية الفكرية بفروعه وتشريعاته المختلفة على مجرد تحديد المصنفات المحمية وتنظيمها، بل تمتد إلى قواعد الحماية المدنية والجنائية، فقانون حقوق المؤلف والحقوق المجاورة فإنه يحمي المواقع الالكترونية إلى جانب المصنفات الأخرى نصت المادة 3 على ما يأتي:

أ-تتمتع بحماية هذا القانون المصنفات المبتكرة في مجالات الآداب، والفنون، والعلوم أيا كان نوعها أو شكلها أو قيمتها أو طريقة التعبير عنها أو الغرض من تأليفها وذلك بمجرد ابتكار المصنف ودون الحاجة إلى أي إجراء شكلي آخر

ب-تشمل الحماية القانونية اليمنيين والأجانب الذين ينتمون إلى الدول الأعضاء في الاتفاقيات والمعاهدات الدولية للملكية الفكرية التي تكون اليمن طرفا فيها وبوجه خاص المصنفات التالية:

1- المصنفات المكتوبة أو المطبوعة كالكتب، والكتيبات، والمجلات، والصحف، والمواقع الالكترونية، والنشرات، وغيرها من المواد المكتوبة

2- المصنفات التي تلْقى شفاها كالمحاضرات، والخطب، والمواعظ.

3- المصنفات الموسيقية سواء كانت مصحوبة بكلمات أم لم تكن

4- مصنفات التصوير الفوتوغرافي وما شابه ذلك

5- المصنفات التمثيلية والمسرحية والمسرحيات الغنائية والموسيقية ومصنفات التمثيل الصامت وتصاميم الرقص

6- المصنفات السمعية والسمعية البصرية.

7- مصنفات الرسم بالخطوط أو بالألوان، والحفر، والزخرفة، والمنحوتات الحجرية، والنقوش المعدنية أو الخشبية، والمفروشات وأية مصنفات أخرى

8- مصنفات الخرائط التخطيطية والمخططات الكروكية.

9- -المصنفات المجسمة المتعلقة بالجغرافيا أو الطبوغرافيا أو العلوم أو العمارة

10- برامج الحاسب الآلي

11- قواعد البيانات إذا كانت مبتكرة من حيث الاختيار أو الترتيب لمحتوياتها

12- عنوان المصنف إذا كان مميزاٍ ومبتكراٍ ولم يكن لفظا جاريا للدلالة على موضوع المصنف.ب-تستفيد من أحكام الفقرة السابقة المصنفات وموضوعات الحقوق المجاورة القائمة وقت صدور هذا القانون شريطة عدم دخولها في الملك العام من قبل وتبين اللائحة القواعد والإجراءات والمواعيد الخاصة بالحماية لهذه المصنفات والحقوق المجاورة وبدء سريانها".(27)

والمشرع اليمني يحمي المخترع المبتكر الذي ابتكر اختراعًا قابل للتطبيق الصناعي أو الزراعي أو في مجال الحرف اليدوية، وصيد الأسماك، والخدمات، نصت المادة 24 من قانة براءة الاختراع على أن: " يحق لأي شخص طبيعي أو اعتباري من اليمنيين أو الأجانب الذين يتخذون لهم مركز نشاط حقيقي في الجمهورية أو في إحدى الدول أو الكيانات التي تربطها بالجمهورية اتفاقية دولية للملكية الفكرية أو تعامل الجمهورية بالمثل حق طلب حماية اختراعه وفقًا لأحكام هذا القانون". (28)

وحيث أن نصوص العقابية التقليدية وضعت في مرحلة سابقة على ظهور هذه الجرائم، فقانون العقوبات مثلا لم يتم تعديله حتى الآن لمواكبة التطور الحاصل في الجرائم الحديثة ومنها الجرائم المعلوماتية.

لكن يمكن الاستعانة بالنصوص الخاصة بالجرائـــم التقليدية لتطبيقها على الجرائم المعلوماتيـــة، في حدود مدى تطويع النصوص العقابية الخاصة بالجرائـــم التقليدية وتطبيقها على الجرائـــم المعلوماتية، وذلك على النحو الآتي:

أولا: القواعد المتعلقة بحماية حرمة الحياة الخاصة:

لم يجد القضاء اليمني بدًا من تطبيق القواعد القانونية التقليدية المتعلقة بجرائم المعلوماتية، لعدم وجود قواعد خاص تحكمها، وقبل أن نقوم بسرد القواعد القانونية المتعلقة بحماية حرمة الحياة الخاصة في قانون العقوبات، نعرج على القواعد الدستورية المعلقة بهذا الجانب.

1- **القواعد الدستورية المتعلقة بحماية حرمة الحياة الخاصة:**

القواعد القانونية في القانون الدستوري الحالي الصادر 2001م المتعلقة بحماية حرمة الحياة الخاصة هي على النحو الآتي:

نصت المادة 1/48 من الدستور على ما يأتي: " تكفل الدولة للمواطنين حريتهم الشخصية وتحافظ على كرامتهم وأمنهم ويحدد القانون الحالات التي تقيد فيها حرية المواطن ولا يجوز تقييد حرية أحد إلا بحكـم من محـكـمـة مختــصـة". ونصت المادة 52من الدستور أيضًا على ما يأتي: " للمساكن ودور العبـادة ودور العلم حرمة ولا يجوز مراقبتها أو تفتيشها إلا في الحالات التي يبينهـا القانـون".

ونصت المادة 53من الدستور أيضًا بأن: "حرية وسرية المواصلات البريدية والهاتفية والبرقية وكافة وسائل الاتصال مكفولة ولا يجـوز مراقبتها أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها إلا في الحالات التي يبينها القانـون وبأمـر قضائــي".

2-**قواعد قانون العقوبات:** (29)

نصت المادة 253 من قانون العقوبات على ما يأتي: "يعاقب بالحبس مدة لا تزيد على سنة أو بالغرامة من دخل مكانا مسكونا أو معدا للسكن أو أحد ملحقاته أو أي محل معدًا لحفظ المال أو عقارًا خلافا لإرادة صاحب الشأن وفي غير الأحوال المبينة في القانون وكذلك من بقي فيه خلافًا لإرادة من له الحق في إخراجه ".

نصت المادة 256من قانون العقوبات على ما يأتي: "يعاقب بالحبس مدة لا تزيد على سنة أو بالغرامة كل من اعتدى على حرمة الحياة الخاصة وذلك بأن ارتكب أحد الافعال الآتية في غير الأحوال المصرح بها قانونًا أو بغير رضا المجني عليه:

استرق السمع أو سجل أو نقل عن طريق جهاز من الاجهزة أيا كان نوعه محادثات جرت في مكان خاص أو عن طريق الهاتف.

التقط أو نقل بجهاز من الاجهزة أيا كان نوعه صورة شخص في مكان خاص.

فإذا صدرت الافعال المشار اليها في الفقرتين السابقتين اثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع فإن رضا هؤلاء يكون مفترضا.

ويعاقب بالحبس مدة لا تزيد على ثلاث سنوات أو بالغرامة الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماد على سلطة وظيفته.

ويحكم في جميع الاحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة كما يحكم بمحو التسجيلات المتحصلة عنها أو إعدامها".

نصت المادة 257 من قانون العقوبات على ما يأتي: "يعاقب بالحبس مدة لا تزيد على سنتين أو بالغرامة كل من أذاع أو سهل إذاعة أو استعمل ولو في غير علانية تسجيلا أو مستندًا متحصلا عليه بإحدى الطرق المبينة بالمدة السابقة أو كان ذلك بغير رضا صاحب الشأن.

ويعاقب بالحبس مدة لا تزيد على ثلاث سنوات كل من هدد بإفشاء أمر من الامور التي تم الحصول عليها بإحدى الطرق المشار إليها لحمل شخص على القيام بعمل أو الامتناع عنه.

ويعاقب بالحبس مدة لا تزيد على خمس سنوات الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتمادًا على سلطة وظيفته.

ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل منها، كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو اعدامها".

ثانيًا: القواعد الخاصة بجرائم الاعتداء على الأموال:

1. جرائم اتلاف المال:

نصت المادة 321 عقوبات على ما يأتي: "يعاقب بالحبس مدة لا تزيد على سنة أو بالغرامة من هدم أو خرب أو أعدم أو اتلف عقارًا أو منقولا أو نباتًا غير مملوك له أو جعله غير صالح للاستعمال أو أضر به أو عطله بأية

كيفيه وتكون العقوبة الحبس مدة لا تتجاوز خمس سنوات إذا اقترفت الجريمة بالقوة أو التهديد أو ارتكبها عدد من الأشخاص أو وقعت في وقت هياج أو فتنه أو كارثه أو نشا عنها تعطيل مرفق عام أو اعمال مصلحة ذات منفعة عامة أو ترتب عليه جعل حياة الناس أو امنهم أو صحته عرضه للخطر وإذا ترتب على الجريمة موت شخص تكون العقوبة الإعدام حدًا ولا يخل ذلك بحق ولي الدم في الدية أو الأرش بحسب الاحوال" .

2- جرائم السرقة:

المـادة 318 من قانون العقوبات: "يعاقب بالحبس مدة لا تزيد على ثلاث سنوات من ضم إلى ملكه مالا منقولا مملوكا للغير سلم اليه بأي وجه". المـادة 294 من قانون العقوبات نصت على أن:" السرقة هي اخذ مال منقول مملوك للغير خفية مما يصح تملكه فاذا وقعت على نصاب من المال في غير شبهة ومن حرز مثله بقصد تملكه دون رضا صاحبه وكان المال المسروق تحت يد صحيحة وبلغ قيمته النصاب المحدد أوجبت الحد الشرعي للسرقة".

3- جرائم خيانة الأمانة:

المـادة 319 من قانون العقوبات نصت على أن: يعاقب بالحبس مدة لا تزيد على سنتين أو بالغرامة من اتلف أو اختلس أو بدد اشياء أو اوراقًا محجوز عليها قضائيًا أو إداريًا أو موضوعة تحت الحراسة ولو حصل ذلك من مالكها".

4- جرائم الاحتيال:

المـادة 310 من قانون العقوبات نصت على أن : " يعاقب بالحبس مدة لا تزيد على ثلاث سنوات أو بالغرامة من توصل بغير حق إلى الحصول على فائدة مادية لنفسه أو لغيره وذلك بالاستعانة بطرق احتيالية (نصب) أو اتخذ اسم كاذب أو صفة غير صحيحة" .

5- جرائم التزوير:

المـادة 210 من قانون العقوبات نصت على أن :" يعاقب بالحبس مدة لا تزيد عن ثلاث سنوات من اصطنع أو زيف ختما أو علامة لأحد الأفراد أو أحدى الجهات أيا كانت أو الشركات المأذونة من قبل الحكومة أو احد البنوك التجارية أو الجمعيات أو الاتحادات أو النقابات أو الأحزاب".

6- جرائم النصب:

المـادة 204 من قانون العقوبات:" يعاقب بالحبس مدة لا تزيد على عشر سنوات كل من صنع أو زيف عمله معدنية أو ورقية متداولة في البلاد قانونا أو في دولة أخرى وكان ذلك بقصد التعامل بها . ويعاقب بذات

العقوبة من لم يساهم في اصطناع العملة أو تزييفها ولكنه مع علمه بحقيقتها ادخلها البلاد أو طرحها في التداول أو حازها بقصد التعامل بها إما من قبل بحسن نية عملة مصطنعة أو مزيفة ثم تعامل بها بهد علمه بحقيقتها فيعاقب بالحبس مدة لا تزيد على ثلاثة أشهر او بالغرامة".

ثالثًا: القواعد الخاصة بجرائم العلانية والنشر:

المـادة 192 من قانون العقوبات نصت على ما يأتي: " يقصد بالعلانية في تطبيق هذا الباب الجهر أو الاذاعة أو النشر أو العرض أو اللصق أو التوزيع على الأشخاص دون تمييز بينهم في مكان عام أو مباح للكافة أو في مكان يستطيع سماعه أو رؤيته من كان موجودًا في مكان عام وذلك بالقول أو الصياح أو الكتابة أو الرسوم أو الصور أو أية وسيلة أخرى من وسائل التعبير عن الفكر. ويعتبر من العلانية مجرد التوزيع على الاشخاص دون تمييز بينهم ولو كان ذلك في مكان غير عام".

المـادة 193 من قانون العقوبات نصت على ما يأتي:" كل من اغرى أو حرض علنا على ارتكاب جريمة أو عدة جرائم فوقعت بناء على ذلك يعتبر شريكا فيها ويعاقب بالعقوبة المقررة لها مالم تكن حدا أو قصاصا فتكون العقوبة الحبس مدة لا تزيد على خمس سنوات أو الغرامة".

المـادة 194 من قانون العقوبات نصت على أن:" يعاقب بالحبس مدة لا تزيد على ثلاث سنوات أو بالغرامة:

اولا: من اذاع علنا اراء تتضمن سخرية أو تحقير الدين في عقائده أو شعائره أو تعاليمه.

ثانيا: من حرض علنا على ازدراء طائفة من الناس أو تغليب طائفة وكان من شان ذلك تكدير السلم العام.

المـادة 195 من قانون العقوبات نصت على ما يأتي:" تكون العقوبة الحبس مدة لا تزيد على خمس سنوات أو الغرامة إذا كان الدين أو المذهب الذي نالته السخرية أو التحقير أو التصغير هو الدين الإسلامي".

المـادة 196 من قانون العقوبات نصت على أن:" لا يعد تحريضا أو إغراء أو تحسينا إذاعة بحث علمي في دين أو مذهب في محاضرة أو مقال أو كتاب بأسلوب علمي هادئ متزن خال من الألفاظ المثيرة وثبت اتجاه المؤلف إلى النقد العلمي الخالص".

المـادة 198 من قانون العقوبات نصت على أن:" يتعاقب بالحبس مدة لا تزيد على سنة أو بغرامة لا تجاوز ألف ريال: ـ

اولا: كل من اذاع أو نشر علنا وبسوء قصد اخبار أو أوراقًا كاذبة أو مزورة أو مختلقة أو منسوبة كذبا إلى الغير إذا كان من شانها تكدير السلم العام أو الإضرار بالصالح العام فإذا ترتب على الإذاعة أو النشر تكدير السلم العام أو الإضرار بالصالح العام ضوعفت العقوبة" .

المـادة 199 من قانون العقوبات نصت على أن:" يعاقب بالحبس مدة لا تزيد على سنتين أو بالغرامة:

اولا: كل من أذاع أو نشر علنًا مطبوعات أو رسومات أو اعلانات أو صور محفورة أو منقوشة أو رسومات يدوية أو فتوغرا فيه أو اشارات رمزية أو غير ذلك من الاشياء أو الصور العامة غذا كانت منافية للآداب العامة .

ثانيا: كل من أعلن عن الاشياء المتقدم ذكرها او عرضها على انظار الجمهور او باعها او اجرها أو عرضها للبيع او الايجار ولو في غير علانية او قدمها علانية بطريقة مباشرة أو غير مباشرة ولو بالمجان وفي اية صوره من الصور او وزعها او سلمها للتوزيع بأية وسيلة علنا او سرا بقصد افساد الاخلاق .

ثالثا: كل من صنع أو حاز بقصد الاتجار أو التوزيع أو الإيجار أو استورد اشياء مما نص عليه فيما تقدم للأغراض المذكورة .

رابعا: كل من جهر علانية باغان أو صياح أو خطب منافية للآداب العامة .

خامسا: كل من اغرى علنًا على الفجور أو نشر اعلانات أو وسائل لهذا الغرض أيا كانت عبارتها.

المـادة 200 من قانون العقوبات نصت على أن:" يعاقب بالحبس مدة لا تزيد على سنتين او بالغرامة كل من: -

اولا: حاز او صنع بقصد الاتجار او التوزيع أو الايجار أو اللصق أو العرض أو عرض بنفسه أو بواسطة غيره علنا أو سرا صورا من شانها الاساءة إلى سمعة البلاد سواء كان ذلك لمخالفة الحقيقة أو تشويهها أو اعطاء وصف غير صحيح أو أبراز مظاهر غير لائقة أو بأية طريقة أخرى .

ثانيا: كل من استورد أو صور أو نقل بنفسه أو بواسطة غيره شيئا مما تقدم للغرض المذكور وكل من أعلن عنه أو عرضه على الانظار أو باعه أو أجره أو عرضه للبيع أو للإيجار ولو في غير علانية وكل من قدمه علانية بالمجان أو وزعه او سلمه.

المــادة 201 من قانون العقوبات نصت على ما يأتي:" إذا ارتكبت الجرائم السابقة عن طريق الصحف يكون رؤساء التحرير والناشرون مسئولين كفاعلين اصليين بمجرد النشر وفي جميع الأحوال التي لا يمكن منها معرفة مرتكب الجريمة يكون المستوردون أو الطابعون أو القائمون بالتوزيع أو اللصق أو العرض مسئولين كفا عليين اصليين."

المــادة 202 من قانون العقوبات نصت على ما يأتي:" يجب ان يحكم في جميع الأحوال بمصادرة الاشياء موضوع الجريمة أو ازالتها وتغلق الدار التي تولت النشر أو العرض مدة لا تتجاوز شهر".

رابعًا: الجرائم الخاصة بإفساد الأخلاق:

المــادة 279 من قانون العقوبات نصت على أن:" يعاقب بالحبس مدة لا تزيد على ثلاث سنوات من حرض غيره على الفجور أو الدعارة فإذا وقعت الجريمة بناء على هذا التحريض تكون العقوبة الحبس الذي لا يتجاوز سبع سنوات".

وإذا كان من حرضه ووقعت منه الجريمة صغيرًا لم يبلغ الخامسة عشر من عمره أو كان المحرض يعول في معيشته على فجور أو دعارة من حرضه يجوز أن تصل عقوبة المحرض إلى الحبس مدة لا تجاوز عشر سنوات. فاذا اجتمعت الحالتان جاز أن تصل عقوبة المحرض الحبس مدة لا تجاوز خمسة عشر سنة".

المــادة 281 من قانون العقوبات نصت على أن:" يعاقب بالحبس مدة لا تزيد على عشر سنوات كل من يدير بيتا أو محلا أيا كان للفجور أو الدعارة ويحكم في جميع الأحوال بغلق البيت أو المحل مدة لا تجاوز سنتين ويحكم كذلك بمصادرة الأثاث والأدوات وغيرها مما كان موجودًا فيه اثناء ممارسة الفجور أو الدعارة".

المــادة 138 من قانون العقوبات نصت على أن:" يعاقب بالحبس مدة لا تزيد على عشر سنوات:

1ـ من عرض للخطر عمدًا وسيلة من وسائل النقل البرية أو البحرية أو الجوية أو عطل سيرها بأية طريقة .

2ـ من عطل بأية طريقة وسيلة من وسائل الاتصال السلكية أو اللاسلكية المخصصة للمنفعة العام

مشروع قانون مكافحة جرائم تقنية المعلومات:

إن مشروع القانون اليمني لمكافحة جرائم تقنية المعلومات المنظور تحت قبة البرلمان بهدف حماية الأمن السيبراني الوطني والمصالح والحقوق العامة والخاصة والآداب العامة، وتعزيز جوانب التعاون الدولي الكفيلة

بمكافحة جرائم تقنية المعلومات، وتعزيز الثقة الدى جمهور مستخدمي تقنية المعلومات بالحماية القانونية للبيانات والمعلومات الالكترونية وتوحيد الجهود لتوفير معايير أمن المعلومات.

فقد أثار هذا المشروع القانوني استخدام مصطلح جرائم تقنية المعلومات، مبررًا ذلك بأن المعلومات هي المعطيات التي تدخل إلى الحاسوب الآلي فقام بحماية هذه المعلومات من أجه عدة، فجرم الأفعال الماسة بتقنية المعلومات فأفرد الفصل الثالث للجرائم الإلكترونية، وحدد عقوباتها، وخص الفرع الأول لجرائم الاعتداء على سلامة وسرية البيانات والمعلومات الالكترونية والمنظومة المعلوماتية. والفرع الثاني تناول فيه الجرائم المرتكبة بواسطة تقنية المعلومات.

الناتج والتوصيات:

النتائج:

تبرز أهمية التشريعات السيبرانية عدة محاور، منها ضرورة وجود إطار تنظيمي وضوابط وإجراءات لتنظيم استخدام وحماية المعلومات المتبادلة على شبكة الانترنت، سواء عبر البريد الإلكتروني أو عبر التطبيقات الأخرى، وذلك بمنع الوسطاء من استخدام هذه المعلومات دون إذن صاحبها أو سوء استخدامها أو وضعها في غير موضعها، من أجل إضفاء صفة الشرعية على التعاملات الإلكترونية، وبيان ضوابطها، ومحدداتها، وحماية المتعاملين عبر الفضاء السيبراني، فقد أمست الحاجة ماسة لإصدار قوانين خاصة بالمعاملات والتجارة الإلكترونية لضمان أمن كافة المعنيين، وتعتبر هذه التشريعات عنصرًا أساسيًا من عناصر البيئة التحتية اللازمة لبناء ثقة المستخدم في خدمات وتطبيقات الفضاء السيبراني، ولدعم وتحفيز التجارة الإلكترونية البيئية محليًا وإقليميًا ودوليًا، خاصة في ظل الاعتماد على الإنترنت كأداة أساسية للقيام بالأعمال التسويقية والتبادلات التجارية.

هذا من جانب ومن جانب آخر فإن هناك محاور أخرى تتطلب تنظيميًا تشريعي لمعالجة وحماية البيانات ذات الطابع الشخصي؛ لأن العديد من التطبيقات الإلكترونية الحكومية والخدمات الإلكترونية المصرفية والصحية تتضمن تخزين بيانات خاصة بالأفراد والمؤسسات في قواعد للبيانات وأنظمة خاصة بهذه التطبيقات، وقد يكون بعض هذه البيانات على مستوى عال من الحساسية أو الخصوصية، لذا فهي بحاجة للحماية عبر قوانين تمنع سوء استخدام هذه المعلومات أو استخدامها دون تصريح أو إذن.

يتطلب تنوع وتشعب قوانين الفضاء السيبراني، خاصة الجانب الفني والتشريعي منها، وجود خبرات متنوعة في اللجان الوطنية الخاصة بصياغة هذه القوانين

المعلومات والاتصالات الآمنة تشكل جزءا لا يتجزأ من عملية بناء مجتمع المعلومات والتنمية الاقتصادية والاجتماعية لجميع الدول. وتشمل تحديات الأمن السيبراني إمكانية النفاذ غير المخول إلى المعلومات المتداولة عبر شبكات تكنولوجيا المعلومات والاتصالات وتدميرها وتعديلها، بحيث يمكن التخفيف من تداعيات هذه التحديات بزيادة الوعي بقضايا الأمن السيبراني، وإقامة شراكات فعالة بين القطاعين العام والخاص، وتبادل أفضل الممارسات الناجحة المستخدمة من جانب صانعي السياسات ودوائر الأعمال وعن طريق التعاون مع أصحاب المصلحة الآخرين.

إن الوصول للمجرم المعلوماتي يشكل عبء فني وتقني بالغ على القائمين بأعمال التتبع للوقائع الإجرامية المختلفة، نظرًا لظهور مشكلة جرائم الكمبيوتر كمشكلة أمنية، وقانونية واجتماعية، فإن الحكومة، وخبراء الأمن، والمهتمين في هذا الموضوع بحاجة إلى تغيير نظرتهم تجاه جرائم الكمبيوتر وبوجه عام في الامور الآتية:

أ- إجاد التشريعات اللازمة لحماية ملكية الكمبيوتر، والبيانات، والمعلومات.
ب- زيادة الوعي الوطني لجرائم الكمبيوتر وللعقوبات المترتبة عليها.
ج- إنشاء وحدات مختصة في التحقيق في جرائم الكمبيوتر في المحاكم وأجهزة الشرطة.
د- إيجاد نوع من التعاون مع الدول الأخرى في الحماية والوقاية من هذه الجرائم.
ه- إدراج الأمن السيبراني من ضمن المناهج التعليمية.

تتطلب صياغة القوانين والتشريعات السيبرانية الإلمام بتجارب بعض الدول وقوانينها السيبرانية، والتعرف على القوانين والتشريعات الدولية المتوفرة لأخذها بعين الاعتبار عند وضع القوانين الوطنية،

أهم التوصيات:

الأمن السيبراني: ضرورة من ضروريات العصر لمواجهة الأخطار السيبرانية.، ولهذا يجب توعية المجتمع بالجرائم السيبرانية ما يترتب عليها من عقوبات

إنشاء منظومة شاملة للتشريعات السيبرانية بحيث تغطي كافة المواضيع المتعلقة باستخدامات الفضاء السيبراني، وتتلاءم مع احتياجات البيئة الرقمية وتطبيقاتها، وتسمح بحماية المستخدم، وتمكن من بناء الثقة

باستخدام الفضاء السيبراني وخدماته، تحتاج عملية سن التشريعات السيبرانية إلى منهج وطني واضح، يعتمد على إشراك كافة الجهات والهيئات والوزارات المعنية

تدريب رجال الشرطة والقضاء على كيفية استخدام أجهزة المعلومات وأدواتها وأشرطتها وآلات الطباعة الخاصة بها والإحاطة بكيفية إساءة استخدامها، وكيفية الكشف عن هذه الجرائم وإثباتها.

حث الدول على التعاون فيما بينها خاصة في مجال المساعدات والإحالة القضائية للكشف عن هذه الجرائم، وجمع الأدلة لإثباتها، وتسليم المجرمين المقترفين لها، وتنفيذ الأحكام الأجنبية الصادرة بالإدانة والعقوبة على رعايا الدولة المقترفين لها بالخارج.

تعزيز وعي أفراد المجتمع حول المخاطر المتعلقة بالإنترنت، وإدراج الأمن السيبراني في البرامج التعليمة الأساسية والعليا ودعم الأبحاث في المؤسسات الأكاديمية، تشجيع المهنيين والطلبة على الانخراط في مجال الأمن السيبراني.

تشجيع المؤسسات على نشر الوعي السيبراني بفاعلية- وتطوير منظومة متكاملة في مجال التدريب في الأمن السيبراني، وتطوير معيار الأمن السيبراني خاص بالشركات الصغيرة والمتوسطة، واستحداث بوابة موحدة للشركات الصغيرة والمتوسطة لتمكينها من تنفيذ المعيار

المشاركة بفعالية في سوق الأمن السيبراني في البلدان العربية. وتقديم إرشادات للحماية من التهديدات السيبرانية الأكثر شيوعا، وتقديم حوافز لتنفيذ الإرشادات الموصى بها.

الحمد لله

تمام كل نعمة

المراجع:

1- القباطي، عبد الجليل، أمن المعلومات في اليمن الواقع والطموح

Jalil@yemen.net.ye

2- القباطي، عبد الجليل، أمن المعلومات في اليمن الموقع والطموح، نفس الموقع.

3- www.differencebetween.net

4- www.computersciencedegreehub.com

5- mamna@kku.sa

6- عبد الأمير، حسين باسم، تحديات الأمن السيبراني، مركز الدراسات الاستراتيجية css، جامعة كربلاء العراق، أيار 2018م، الموقع

kerbalacss.uokerbala.edu.iq/wp/blog

7- فريد، نائلة عادل محمد، الجرائم المعلوماتية على شبكة الإنترنت، لبنان منشورات الحلبي الحقوقية، 2005م، ص28 وما بعدها.

8- يوسف، يوسف حسن، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، مصر، ط1، 2011م، ص13.

9- حجازي، عبد الفتاح بيومي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي، دار الكتب العربية، مصر، ط1، 2007م، ص24.

10- محمد، آمنة على البشير، الأمن السيبراني في ضوء مقاصد الشريعة، المجلد الأول من العدد السابع والثلاثون لمجلة كلية الدراسات الإسلامية والعربية للبنات بالإسكندرية، ص460.

mamna@kku.edu.sa https://edu.moe.gov.sa/jeddah

11- المومني، نهلا عبد القادر، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، ط1، 1429هـ 2008م، ص20.

12- إبراهيم، خالد ممدوح، الجريمة المعلوماتية، دار الفكر العربي، الإسكندرية، ط1، 2009م، ص77 وما بعدها.

13- البورسعيدي، هلال بن محمد بن حارب، الحماية القانونية والفنية لقواعد المعلومات المحوسبة، دار النهضة العربية، القاهرة، 2009م، ص35 وما بعدها. مصطفى، أحمد محمود، جرائم الحاسبات الآلية في التشريع المصري، دار النهضة العربية، القاهرة، ط1، 2010م، ص18.

14- حجازي، عبد الفتاح بيومي، النظام القانوني لحماية الحكومة الإلكترونية، الكتاب الثاني، الحماية الجنائية والمعلوماتية نظام الحكومة الالكترونية، دار الفكر الجامعي، بالإسكندرية، ط1، 2003م، ص7.

15- الحمامي، عمر أبو الفتوح عبد العظيم، الحماية الجنائية للمعلومات المسجلة إلكترونًا، دراسة مقارنة، دار النهضة العربية، القاهرة، 2010م، ص142.

16- الصغير، جميل عبد الباقي، القانون الجنائي، والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، 1992م ص4. الشوا، محمد سامي، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1998م، ص31. ابن يونس، عمر محمد، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، القاهرة، ط2004،1م، ص5. رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994م، ص5 وما بعدها. سلامة، أحمد عبد الكريم، قانون حماية البيئة، دراسة تأصيلية في الأنظمة الوطنية والاتفاقية، الطبعة الأولى، منشورات جامعة الملك سعود، السعودية، 1418هـ 1997م، ص535. حجازي، عبد الفتاح بيومي، حقوق المؤلف في القانون المقارن، بهجات للطباعة والتجليد، مصر، 2009م، ص79.

17- المادة 3 من مشروع قانون مكافحة جرائم تقنية المعلومات اليمني، المنظور تحت قبة البرلمان.

18- https://ar.wikipedia.org › wiki

19- http://www.escwa.un.org/divisions/div_editor/Download.asp?table_name=divisions_other_ar&field_name=ID&File(10) ID=251.

http://isper.escwa.un.org/RegionalActionPlans/ArabICTStrategy/StrategyDocument/tabid/70/language/ar-LB/Default.aspx

20- http://isper.escwa.un.org/FocusAreas/CyberLegislation/Projects/tabid/161/language/en-US/Default.aspx

اجتماع الخبراء حول تنسيق التشريعات السيبرانية في المنطقة العربية (بيروت، 16-17شباط/فبراير، 2011م)

http://www.escwa.un.org/information/meetingdetails.asp?referenceNum=1427E

21- http://www.escwa.un.org/ information/meetingdetails.asp?referenceNum=2002E

22- موقع وزارة الاتصالات وتقنية المعلومات اليمنية https://www.mtit.gov.ye

23- https://www.almarrakchi.com

24- القانون المدني رقم 14 لسنة 2002م، الجريدة الرسمية العدد 7 ج1 لسنة 2002م.

25- المادة 2 من القانون رقم 40 لسنة 2006م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية. الجريدة الرسمية العدد 24 لسنة 2006م.

26- المادة 4 من القانون رقم 13 لسنة 2012م بشأن حق الحصول على المعلومات. الجريدة الرسمية العدد 13ج1 لسنة 2012م.

27- القانون رقم 15 لسنة 2012م بشأن حماية حق المؤلف والحقوق المجاورة. الجريدة الرسمية 14لسنة 2012م.

القانون رقم 2 لسنة 2011م بشأن براءة الاختراعات ونماذج المنفعة وتصميمات الدوائر المتكاملة المعلومات غير المفصح عنها. الجريدة الرسمية العدد1ج1 لسنة 2011م.

28- القـرار جمهوري بالقانون رقم 12لسنة 1994م بشـأن الجرائم والعقوبات. الجريدة الرسمية العدد 19 ج2 لسنة1994م.

خطر الإرهاب السيبراني

الدكتور عماد عواد
سفيـــــر سابــق، مستشار في المجلس القومي لحقوق الإنسان- (مصر)

الملخص:

في الوقت الذي يتم فيه مناقشة ملف الأمن السيبيراني في التشريعات العربية، يلزم تخصيص جزء من الوقت لضبط المفاهيم والتمييز بين عدة مصطلحات من قبل الأمن السيبراني، أمن المعلومات، الإرهاب السيبراني...ألخ. وتهدف هذه الورقة إلى توضيح المخاطر التي يمثلها هذا النوع من الإرهاب مقارنة بما يتم التعامل معه حالياً من جرائم اليكترونية حيث أن الأمر يتعلق بمهاجمة الأجهزة والشبكات إما بغرض تعطيلها أو تشويه المعلومات داخلها، أو إخراجها عن نطاق الخدمة. وعلى الرغم من انه تم الإعلان عن القضاء على المعاقل الأخيرة لتنظيم "الدولة الإسلامية" وتصفية زعيمها، إلا أن هناك العديد من العناصر التي تشير إلى احتمال أن هذا التنظيم قد استفاد من فترة انشغال العالم بالتصدي لفيروس كوفيد 19 لإعادة ترتيب صفوفه وربما الاستعداد لاقتحام هذا التنظيم مجال الإرهاب السيراني لما له من قدرة معرفية فائقة في مجال الإنترنيت. وإزاء هذا الاحتمال يلزم اتخاذ العديد من الخطوات الوقائية على كل من المستوى العربي والعالمي.

Abstract

While it is time to discuss the file of Cyber Security in Arab Legislations, it becomes highly important to fix certain expressions such as: cyber Security, Information Security, electronic crimes and cybercrimes.

This paper aims at clarifying the enormous dangers that cyber terrorism implies in comparison of the traditional or even electronic terrorism. In fact, the target here is different, it's simply the networks and the cyber space itself. Moreover, the objective is also different, while in electronic crimes we try to steal information, in cyber-attacks the objective is to destroy information or the system or even both of them.

Despite the fact the State of Khalifah, created by Daesh, has been destroyed and if commander physically eliminates, one can't exclude a return in force of such group, after having recognized its ranges while the whole world was trying to stop the spread of Corvid-19 virus. Consequently, the scenario of a cyber-terrorism operation to take place can't be simply excluded.

مقدمة

يعتبر ملف الإرهاب من الملفات التي طرحت نفسها منذ بداية العقد الحالي، بداية بأحداث الحادي عشر من سبتمبر 2001 وما أعقابها من إعلان الولايات المتحدة الأمريكية ما أطلقت عليه الحرب على الإرهاب والذي مثله آنذاك تنظيم القاعدة التي سارع بالتفاخر بإنجازاته وأصدر تحذيراته المتعاقبة للغرب، معلناً بدورة الحرب ضد الصليبيين والصهيونيين. وعلى الرغم من أن هذه الحرب لم يكن لها مسرح عمليات محدد إلا أنه الجهود العسكرية الأمريكية وما تم تدشينه من تحالف دولي ضد الإرهاب ركزت على أفغانستان في البداية، بحكم تواجد تنظيم القاعدة هناك بكثافة، إلا أنه بعد ذلك اتسع نطاق المواجهة وأصبح يشمل كافة أرجاء العالم، حيث نحج التنظيم في أن ينتقل من موقع إلى أخر في العالم لتوجيه ضرباته ولينتشر تحت مسميات مختلفة: تنظيم القاعدة في شبة الجزيرة العربية، تنظيم القاعدة في الشام والعراق، تنظيم القاعدة في شمال أفريقيا...الخ.

إلا أنه سرعان ما حدث تغير مفاجئ مع الإعلان في عام 2014 عن تأسيسي ما أطلق عليه "تنظم الدولة الإسلامية" والذي أعلن عن قيام "الخلافة الإسلامية" واتخذ من أجزاء من العراق وسوريا مركزاً له معلناً إياها دولة، ليعلن البدء في مرحلة جديدة استثمر فيها التنظيم الوليد بمهارة شبكة الإنترنيت لتحقيق العديد من الأهداف التي كان من الصعب عليه تحقيقها بالوسائل التقليدية، ومن بينها تمكنه من جذب عدد لا بأس به من المقاتلين الأجانب من أكثر من مائة دولة في العالم. ولم يتوقف الحديث عن سعي التنظيمات الجهادية المتطرفة إلى الحصول على أسلحة دمار شامل من دول أوروبا الشرقية التي كانت تابعة للاتحاد السوفيتي، وأعقب ذلك ترددت شائعات عن تطلعها إلى الحصول على مواد تستخدم في الحروب الكيميائية أو البيولوجية، وأخيراً يدور النقاش الآن حول مدي قدرة تلك التنظيمات، خاصة تنظيم "الدولة الإسلامية/داعش" الانخراط في مجال الإرهاب السيبراني بعدما اثبته من قدرات فائقة في استثمار شبكة الإنترنيت لتحقيق أهداف كان من الصعب تحقيقها في ظل تضييق الرقابة الأمنية على عملية الاتصال المباشر بالأفراد والتجمعات بغرض التجنيد أو الحصول على التمويل.

أهمية الدراسة:

تكتسب هذه الدراسة أهمية كبيرة على المستويين العملية والنظري. فمن الناحية العملية هناك على الأقل عاملين يلزم أخذهما بعين الاعتبار: يتمثل العامل الأول في أن الدراسة تتناول ملفاً على درجة عالية من الأهمية لم يثبت بعد أنه تم الانتهاء منه بشكل تام، وإنما ما حدث على وجه التحديد هو القضاء على معاقل ما أطلق عليه "دولة الخلافة" في كل من سوريا والعراق، وتصفية زعيم تنظيم "الدولة الإسلامية/داعش" جسدياً كما كان عليه الحال بالنسبة لزعيم القاعدة، أسامة بن لادن، قبله. فعلي الرغم من كل ذلك استمرت تحذيرات الخبراء والتخصصين ووكالات الاستخبارات من أن الإرهاب لم يتم دحره وأن القضاء على هذا التنظيم أو ذاك لا يعنى القضاء على الظاهرة التي أضحت لها جذور في أماكن عديدة من العالم وتتخذ أشكالاً مختلفة سواء في شكل "الإسلاموفوبيا" والتي تقود إلى جرائم الكراهية أو التنظيمات الإسلامية المتطرفة والتي نفذت عمليات دامية في مواقع كثيرة من العالم. أما العامل الثاني فإنه يدور حول القدرات الكبيرة والمهارات العالية التي اظهرتها بعض هذه التنظيمات، وعلى الأخص تنظيم "الدولة الإسلامية/داعش" في استخدام شبكة الإنترنيت، مما يدفع على التخوف من إمكانية توظيف تلك القدرات، عندما يحين الوقت، بطرق مستحدثة تطرح الإرهاب في ثوبه الجديد، ألا وهو "الإرهاب السيبراني"، خاصة مع تملكها اللازمة، وما سجلته من قبل من بعض النجاحات في هذا المجال.

وعلى المستوي النظري، فإن هذه الدراسة تأتي لتضيف إلى غيرها من الدراسات التي كشفت عن وجود ثغرات في قوانين تم إصدارها للتعامل مع جرائم تقنية المعلومات والجرائم الإليكترونية، مما يتطلب التوصية بسد الثغرات الموجودة في هذه التشريعات لتكون قادرة على التعامل مع التحديات التي تفرضها الجريمة التي نحن بصدد التعامل معها والتي لها صفاتها وخصائصها التي تميزها عن غيرها من الجرائم. كما يمكن أن تكون هذه الدراسة بداية لدراسات أكثر تعمقاً حول هذه الظاهرة الخطيرة التي قد تفرض نفسها فجأة على المسرح الدولي في وقت لازال فيه العالم يحاول التصدي لجائحة كوفيد-19 وصوره المستجدة.

إشكالية الدراسة:

تتميل إشكالية الدراسة في الخلط الدائر بين العديد من المصطلحات، فهناك من يتحدث عن الجرائم الإليكترونية، وآخر يتناول جرائم تقنية المعلومات، وثالث يشير إلى الجريمة السيبرانية. ووسط هذه الخلط يكون من الطبيعي عدم القدرة على وضع تشريع يتعامل مع مجموعات مختلفة من الجرائم يجمع بينها فقط

استخدامها لشبكة الإنترنيت كمجال للتحرك وجهاز الكومبيوتر كأداة للتنفيذ. وفي هذا السياق كان من الضروري تمييز الجريمة السيبرانية عن غيرها من الجرائم واعطائها مكانها الذي يتناسب مع حجم خطورتها

منهج الدراسة:

يُعتبر المنهج الوصفي التحليلي من أنسب المناهج للتعامل مع هذا الموضوع؛ حيث يتعلق الأمر بتعريف المخاطر وتوضيح خصائصها، ويستعرض خبرتها التي مازالت ماثلة في الأذهان، وما يمكن أن تصل إليه عبر استغلال ما تركته ورائها من أرث سواء في شكل "المدربين الافتراضيين" أو "الخلايا النائمة" فيما يتعلق بالتنظيمات الإسلامية المتطرفة، أو بالجهود التي يبذلها اليمين المتطرف في تكثيف اعتداءاته على المجتمعات الإسلامية المقيمة في الغرب والتي تشكل جزءً لا يتجزأ منه.

خطة الدراسة:

- **المبحث الأول: الإنترنيت والإرهاب العابر للحدود**
  - المطلب الأول: خبرة تنظيم الدولة الإسلامية
  - المطلب الثاني: قدرات اليمين المتطرف
- **المبحث الثاني: الإرهاب السيبراني**
  - المطلب الأول: ضبط المفاهيم وتحديد المضمون.
  - المطلب الثاني: احتمالات صعود الإرهاب السيبراني.

الخاتمة: النتائج والتوصيات

المبحث الأول: الإنترنيت والإرهاب العابر للحدود

المطلب الأول: خبرة "تنظيم الدولة الإسلامية/داعش"

شأنها في ذلك شأن كافة أشكال الجريمة المنظمة، سعت التنظيمات الإرهابية إلى تحقيق أقصي استفادة ممكنه من العولمة لحقيق مآربها من خلال تجاوز حدود الدول واضفاء طابع عالمي على تحركاتها، مستغلة في ذلك ما وفره التطور الضخم في تكنولوجيا المعلومات من قدرات فاقت بكثير ما كان متاح من قبل في العديد من المجالات، سواء من حيث سرعة الاتصال أو سهولته أو ما يوفره من وسائل تأمين ضخمة.

فمن جانب، أدركت التنظيمات الإرهابية انه يمكنها من خلال شبكة الإنترنيت أن تنشر أفكارها وأطروحاتها بطرق مختلفة تتناسب مع الشرائح المستهدفة، وبلغات متعدد تخاطب الإنسان في أي مكان وجد. ومن جانب آخر، سمحت وسائل التواصل الاجتماعي بتوفير خاصية التكرار المستمر لمضمون الرسائل التي تبعث بها هذه التنظيمات والتواجد بشكل مستمر على الساحة على مدار الساعة؛ حيث يتم تناقلها من شخص إلى مجموعة، ومن كل شخص داخل المجموعة إلى مجموعته ومن كل مجموعة إلى المجموعات الأخرى وهكذا إلى ما لانهاية. وفصلاً عما تقدم، تمكنت تلك التنظيمات من الحصول على قدر من التأمين لم تكن تحظ به مسبقًا، في ضوء ما وفرته شبكة الإنترنيت من فضاء افتراضي يمكن للأطراف الولوج والخروج منه بسهولة ويسر مع الاحتماء ببرامج تمكنه من التخفي وإخفاء الأثر، ومن شأن كل هذا أن يضع المزيد من العراقيل أمام عمليات الرصد والمتابعة من قبل أجهزة الأمن المعنية، بل ويجعلها مستحيلة في بعض الحالات وإن كان ذلك لفترات محدودة، وإن كانت كفاية لتمكين خبراء تكنولوجيا المعلومات الذين يعملون لحساب التنظيمات الإرهابية من الانتقال إلى مواقع أكثر أمناً.

في ضوء ما تقدم، اكتسبت ظاهرة الإرهاب أبعادًا غير مسبوقة؛ حيث تمكنت تنظيمات جهادية متطرفة تمتلك قدرات فنية عالية، من المناورة بمهارة فائقة في ثنايا العالم الافتراضي؛ ما مكنها من أن تفرض نفسها كخطر مُدمر قد يحل بأي مكان وفي أي توقيت، قادر على توجيه ضربات وتحقيق أهداف كان يصعب عليه القيام بها في السابق بالأساليب والأدوات التقليدية التي جعلته على الدوام في مرمي الاستهداف من قبل الأجهزة الأمنية. فانطلاقاً من المنصات الإليكترونية أصبحت التنظيمات الإرهابية، المؤهلة فنياً، قادرة على التواصل والتفاعل مع الجمهور المستهدف بكافة مستوياته بسهولة وسرعة فائقة مع تقليل هامش المخاطرة إلى أقصي درجاته. وقد دفعت هذه الوضعية المثيرة البعض إلى طرح مقولة مفادها أن الانترنيت أصبح شريكًا في صناعة الإرهاب في العالم؛ [22] حيث يلعب دوراً مؤثراً في صناعة التطرف والترويج للتفسيرات الدينية والآراء الفقهية المضللة، مما سهل عملية استقطاب العناصر المؤهلة للانحراف؛ والتحريض على العنف؛ وتوفير الإرشادات العملية لتصنيع المتفجرات واستخدامها؛ وتزويد العناصر الإرهابية بوسائل سهلة وآمنة للتواصل.

---

[22] **محمد الحمامصي، "الانترنيت شرك في صناعة الإرهاب في العالم"، (لندن: موقع جريدة العرب، 2015/2/2). تاريخ الاطلاع 29 نوفمبر 2018.**

https://alarab.co.uk/الإنترنت-شريك-صناعة-الإرهاب-في-العالم

في هذا السياق، تمكنت تنظيمات من قبل "تنظيم الدولة الإسلامية/داعش" عبر شبكة الإنترنيت من تجنيد مقاتلين من كافة بقاع العالم وإرشادهم إلى طرق الوصول إلى مواقع التمركز ونقاط الاشتباك ليضخموا صفوفها مشكلين ما تم التعارف على تسميته بــ "المقاتلين الأجانب". وفي حالات أخرى، اقتصر تأثير هذه التنظيمات على تشبيع الأشخاص بأفكارها بالرغم من بقائهم في بلادهم، وتظل هذه العناصر تتحين الفرصة للانتقال من مستوى الأفكار المجردة إلى التحرك العملي على أرض الواقع بتنفيذ هجمات فردية من الداخل فيما عرف بمصطلح "الذئاب المنفردة".

في واقع الأمر، تمكنت التنظيمات الإرهابية ذات الطبيعة الدينية المتطرفة، وفي مقدمتها "تنظيم الدولة الإسلامية/داعش" من استثمار قدراتها ومهارة أنصارها المتخصصين في هذا المجال والقادمين من كافة بقاع العالم من أجل القيام بالعديد من الوظائف؛ قسمها مكتب الأمم المتحدة المعني بالمخدرات والجريمة المنظمة، بالتعاون مع فرقة العمل التابعة للأمم المتحدة المعنية بتنفيذ مكافحة الإرهاب، إلى فئات تتداخل في بعض الأحيان وهي: الدعاية (بما يشمل التجنيد، والدفع باتجاه التطرف، والتحريض على الإرهاب) والتدريب والتخطيط (بما يتضمن التخطيط عبر الاتصالات السرية والمعلومات المستمدة من مصادر علنية)...الخ. [23]

في تقريره بعنوان: "استخدام الإنترنيت ووسائط التواصل الاجتماعي بوصفها أداة للترويج والتجنيد" المقُدم لمجلس الأمن في شهر كانون الثاني/يناير عام 2016، ركز الأمين العام للأمم المتحدة على تزايد خطورة التهديد الذي يشكله تنظيم "الدولة الإسلامية" بفعل التطور التكنولوجي المتنامي الذي تتسم به هذه الجماعة؛ حيث أوضح أن التنظيم يلجأ بشكل متزايد إلى الإنترنت ووسائط التواصل الاجتماعي بغية إيصال رسائله إلى من يحتمل تجنيدهم. وذهب التقرير إلى حد القول بأنه يبدو أن التنظيم تمكن من إنشاء نظام قوي ومنخفض التكلفة لبث دعايته، وتحديد من يحتمل تجنيدهم، وتخصيص الموارد البشرية من أجل إقناع الأفراد المستهدفين بالانضمام إلى صفوفه. ما تسبب في زيادة نمو عدد المقاتلين الإرهابيين الأجانب الذين يسافرون إلى الجمهورية العربية السورية والعراق. كما ركز الأمين العام على القدرات الخاصة للتنظيم في مجالين: الأول هو مرونة الحركة والانتقال من أداة إلى أخرى من أدوات التواصل الاجتماعي، كي يتماشى مع الجهود المبذولة لإغلاق قنوات تواصله مع الجمهور. والثاني يتصل بالقدرة على تكييف مواصفات رسائله المنشورة على شبكة الإنترنيت وفقاً للجمهور المستهدف. فوفقاً لما أورده التقرير تضمنت أشرطة الفيديو التي بثها هذا التنظيم

([23])https://www.unodc.org/documents/congress/backgroundinformation/Terrorism/Use_of_the_Internet_for_Terrorist_Purposes_Arabic.pdf

خلال العامين السابقتين على صدور التقرير الموضوعات التالية: أعمال حربية 30%؛ مقابلات مع المجاهدين 25%؛ وصور تبين التنظيم كـ"دولة مثالية" تؤدي مهامها 18%؛ عمليات إعدام 15%؛ أما المواضيع الدينية البحتة فقد كانت أقل شيوعا. وكثيرا ما كانت أشرطة الفيديو مُعدَّة بشكل جيد ومستوحاة من أفلام الإثارة وألعاب الفيديو.

كذلك أكد التقرير على أن هذا النهج لم يقتصر فقط على اجتذاب الشباب الساعين إلى القتال فحسب، بل أيضا هدف كذلك إلى استقطاب اصحاب المهن من قبيل الأطباء والمهندسين وأخصائي تكنولوجيات المعلومات والاتصالات، فضلاً عن النساء والفتيات. كما اقترنت حملات تمييز الأنشطة والترويج التي يقوم بها تنظيم الدولة الإسلامية بحملات ذات مواصفات فردية لزرع التطرف والتجنيد يقوم بها مهيؤون مدربون تدريبا جيدا باستخدام تطبيقات الدردشة المباشرة والتداول بالفيديو وغيرها من أدوات تكنولوجيا المعلومات والاتصالات.

حول هذه النقطة، أوضح مكتب الأمم المتحدة المعني بالمخدرات والجريمة، في منشوره الذي أعده بالتعاون مع فرقة العمل التابعة للأمم المتحدة المعنية بتنفيذ تدابير مكافحة الإرهاب: "أن أكبر خطر تشكله الدعاية الإرهابية يتعلق بالطريقة التي تُستخدم بها والقصد الذي تُبث من أجله. فالدعاية الإرهابية التي توزع عبر الإنترنيت تشمل مجموعة واسعة من الأهداف وتوجه إلى مختلف أنواع الجماهير. فقد تُصمم الدعاية خصيصاً من أجل المؤيدين المحتملين أو الفعليين لتنظيم من التنظيمات أو لأحد المعتقدات المتطرفة المشتركة، أو من أجل معارضي هذا التنظيم أو المعتقد، أو من أجل الضحايا المباشرين أو غير المباشرين لأعمال إرهابية، أو من أجل المجتمع الدولي أو جزء منه، في جملة موضوعات أخرى. وقد تركز الدعاية التي تستهدف المؤيدين المحتملين أو الفعليين على التجنيد، والدفع باتجاه التطرف، والتحريض على الإرهاب، عبر رسائل تعبر عن مشاعر الفخر والاعتزاز بتحقيق الأهداف المرسومة والتفاني من أجل تحقيق هدف متطرف.

كما يمكن أن تستخدم هذه الدعاية لإثبات النجاح في تنفيذ هجمات إرهابية لمن قدم دعماً مالياً لمنفذي هذه الأعمال. وقد تشمل الأهداف الأخرى للدعاية الإرهابية التأثير على نفسية الفرد لإضعاف إيمانه ببعض القيم الاجتماعية الجماعية، أو لبث شعور بالقلق الزائد أو الخوف أو الذعر في مجتمع من المجتمعات أو شريحة منه.

وقد يتأتى ذلك عبر نشر معلومات مضللة، أو شائعات أو تهديد باستخدام العنف، أو صور لأعمال عنف تثير المشاع، وقد يشمل الجمهور المستهدف أولئك الذين يشاهدون المواد الدعائية مباشرة، فضلاً عمن يتأثرون بالإشاعات التي قد تنتشر بسبب هذه المواد. وفيما يخص المجتمع الدولي بشكل عام، فإن الهدف من الدعاية غالباً ما يكون إعطاء الانطباع بأن القائمين عليها يسعون لتحقيق غايات سياسية نبيلة". [24]

المطلب الثاني: قدرات اليمين المتطرف

نتيجة للتطور الهائل في التكنولوجيا وما ترتب عليه من ظهور الإعلام الجديد، الذي استخدمه التنظيمات الإرهابية التي تدعي انتماءها للإسلام، كان من الطبيعي أن تقوم التجمعات اليمنية المتطرفة في الدول الغربية، بالنشر على نطاق واسع لصورة نمطية سلبية (إرهابية) عن المسلم، إلى الحد الذي دفع بالبعض لطرح مفهوم "الصورة الانشطارية" ويقصد بذلك تشظي الصورة النمطية وانتشارها في كافة الاتجاهات، وما ينتج عن ذلك من صورة ضبابية مبعثرة ليس من السهل على أي مجتمع التخلص منها. [25]

يُشار في هذا الخصوص إلى أن مرتكبي العمليات ضد المسلمين والعرب يتم تقديمهم بطريقة مختلفة عن أولئك المسلمين أو العرب الذين يرتكبون عمليات مشابهة. فعلي حين يُنظر عادة إلى الفئة الأولي نظرة أقل تشدداً ويتم توصيف العملية بشكل مخفف في إطار ما يُطلق عليه جرائم الكراهية، يتم التعامل مع الفئة الثانية، في معظم الأحيان وبشكل تلقائي، على أنها جرائم إرهابية.

وقد كانت الولايات المتحدة الأمريكية مسرحاً لظهور العديد من الجماعات والحركات ارتكبت انتهاكات وجرائم تدخل في إطار التصنيف الوارد في نص المادة (19) من العهد الدولي الخاص بالحقوق المدنية والسياسية من جانب، والمادة (2) من اتفاقية مكافحة التمييز العنصري.

وفي واقع الأمر قامت هذه الحركات على مفاهيم عنصرية ترفض الآخر وتهدف إلى اقصائه، بدءً بجماعة كو كولوكس كلان (1866)، وانتهاءً بالجماعات التي تعتبر نفسها من الحركات النازية الجديدة، التي لم

([24])https://www.unodc.org/documents/congress/backgroundinformation/Terrorism/Use_of_the_Internet_for_Terrorist_Purposes_Arabic.pdf

[25] **شاكر نوري، "الإرهاب في الإعلام الفرنسي... من الصورة النمطية إلى الصورة الانفجارية"، (موقع نزوة: 17 يناير 2018)، تاريخ الاطلاع 28 نوفمبر 2018.**

https://www.nizwa.com/الإرهاب-فـي-الإعلام-الفرنسي-من-الصورة/

يقتصر وجودها على الكثير من الولايات في أمريكا وإنما امتد إلى القارة الأوربية، فقد برع أنصارها- بدورهم- في استخدام شبكة الإنترنيت للترويج لأفكارهم فضلاً عن المذياع وخدمات الأخبار المخصّصة للعنصريين البيض، كما يعقدون مؤتمرات علنية في مُدن مختلفة في الولايات المتحدة، ويقودون حملة غير مسبوقة لزيادة حجم الدعم لهم، لا سيّما لدى العنصريين الحليقي الرؤوس. وأضحت الحركة، التي تتخذ من مينيا بوليس مقراً لها، منظمة بث الكراهية الأكبر في الولايات المتحدة. [26]

لم تقتصر جرائم الكراهية فقط على الولايات المتحدة الأمريكية وإنما تسارعت وتيرتها في القارة الأوروبية نتيجة لمجموعة من العوامل أبرزها انتشار خطابات الكراهية على الفضاء الافتراضي، وفي هذا الخصوص ربطت دراسة في يناير 2018 أجراها عدد من الباحثين في جامعة "وارويك" البريطانية بين الاعتداءات التي يتعرض لها المسلمون واللاجئون في ألمانيا والولايات المتحدة وخطابات الكراهية التي تُروج لها مواقع التواصل الاجتماعي. وعلى سبيل المثال توصلت الدراسة، من خلال تحليل خطابات أعضاء حزب "البديل من أجل ألمانيا" اليميني الشعبوى على موقع فيسبوك إلى وجود علاقة وثيقة بين هذه الخطابات، وتكرار الاعتداءات على المسلمين واللاجئين. أما فيما يتصل بالولايات المتحدة فقد لاحظت الدراسة تزايد حالات الاعتداءات على الأقليات عقب تغريدات المرشح، ثم الرئيس، دونالد ترامب التي تستهدف الأقليات.

يضاف إلى ذلك أنشطة الجماعات المتطرفة في بريطانيا من قبيل Britain First و First Generation Identity وNational Action إضافة إلى وجود شخصيات إعلامية معروفها بتوجهاتها اليمينية المتطرفة ونشاطها على وسائل التواصل الاجتماعي الذي يحظى بعدد كبير من المشاهدات من قبيل: ستيفن لينون (المعروف باسم تومي روبنسون) و بول جوزيف واتسون، فضلاً عن كاتي أوليفيا هوبكنز التي نشرت مقالاتها في عدد من الصحف البريطانية، وقد اضطرت صحيفة الديلي ميل إلى دفع مبلغ 150 ألف جنية إسترليني لعائلة مسلمة بعد قيام هوبكنز باتهامها بالتطرف عقب نشرها تغريدات لها في تويتر بعد حادثة مانشستر إرينا عام 2017، وقد انضمت في يناير 2018 إلى جماعة نازية كندية.

([26]) عامر دكة، "النازيون الجدد يطلون برؤوسهم في الولايات المتحدة"، (موقع المصدر: 23 نوفمبر 2016) تاريخ الاطلاع 29 نوفمبر 2018.

https://www.al-masdar.net/النازيون-الجدد-يطلون-برؤوسهم-في-الولا

المبحث الثاني: الإرهاب السيبراني

المطلب الأول: ضبط المفاهيم وتحديد المضمون

يقود استخدام مصطلح الإرهاب السيبراني إلى التفكير في احتمال حدوث تغيير جذري في أساليب الإرهاب المعروفة حتى الآن، فلقد كان واضحاً من العرض السابق توفر قدرة على استخدام شبكة المعلومات في الترويج للأفكار المتطرفة والتجنيد وجمع الأموال ونشر الأفكار وإعطاء التعليمات والتوجيهات لتنفيذ عمليات محددة في أوقات ومناطق متفق عليها. إلا أن التطرق إلى مفهوم الإرهاب السيبراني يعنى الارتقاء إلى مستوى أكثر تقدماً في سلم التهديدات؛ يتم فيه استخدام الفضاء السيبراني، وهو ما يمثل بيئة تفاعليه افتراضية مرتبطة بمجموعة من الأجهزة الرقمية والشبكات والبرمجيات، لتحقيق عمليات ذات طابع إرهابي تمس في الجوهر مكونات هذه البيئة، بمعنى الأجهزة والشبكات والبرمجيات.

يلزم من البداية الإشارة إلى وجود خلط كبير في المفاهيم عندما نصل إلى هذه النقطة، حيث يتم الحديث عن الجريمة الإليكترونية، وأمن المعلومات، والأمن السيبراني، باعتبارهم مترادفات لشيء واحد نظراً لاشتراكهم جميعاً في الأداة (الحاسب الآلي) والمسرح (الفضاء الافتراضي). غير أن الأمر لا يمكن التسليم به بهذه السهولة عندما يدور الحديث عن الإرهاب السيبراني، ومن ثم يلزم تحديد مفهوم الأمن السيبراني كنقطة انطلاق لفهم الإرهاب السيبراني.

تعددت التعريفات التي تم تقديمها لتوضيح هذا المفهوم، وفي هذا الخصوص نشير إلى أن وزارة الدفاع الأمريكية أشارت إليه باعتباره: "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم: الهجمات، التخريب، التجسس والحوادث." ومن جانبه عرفة الإعلان الأوروبي بأنه:

"قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات[27]." أما مكتب التحقيقات الفيدرالي الأمريكي فإنه قدم الإرهاب السيبراني على أنه: "الهجوم المتعمد ذو الدوافع السياسية ضد أنظمة المعلومات، وبرامج الكمبيوتر والبيانات المخزنة من قبل مختلف الفاعلين. وهو التهديد أو الهجوم غير القانوني

---

[27] الموسوعة السياسية، الرابط

https://political-encyclopedia.org/

بشن هجمات على أجهزة الكمبيوتر، وأنظمة المعلمات، والبرامج، والبيانات، بهدف ترهيب وإكراه الحكومات تحقيقاً لأهداف مختلفة".[28]

وبشكل عام، يمكن القول إن الأمن السيبراني يُقصد به مجموعة الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية البرمجيات وأجهزة الكمبيوتر والفضاء السيبراني بشكل عام زون مختلف الهجمات والاختراقات والتهديدات السيبرانية.[29] وانطلاقاً من هذا التعريف يبدو واضحاً ان الأمن السيبراني يشير إلى مفهوم أوسع من ذلك الخاص بأمن المعلومات والتي قد تكون معلومات ملموسة في صيغة مكتوبة لا تدخل في دائرة اهتمام الأمن السيبراني على الإطلاق. في المقابل، يمكن اعتبار التزوير الإليكتروني صورة من صورة الاختراق للأمن السيبراني حيث يتمكن الطرف الراغب في تزوير المستند من اختراق نظام الأمان الذي يحيط بالمعلومات في إطار شبكة اليكترونية تخدم حاسب آلي، ويغير المعلومات التي يرغب في تغييرها باستخدام أدوات اليكترونية، ثم يخرج من الموقع دون أن يترك ورائه أثر.

وفي حقيقة الأمر، فإنه نظراً لعدم وجود تعريف دقيق في هذا المجال، يذهب البعض إلى التمييز بين نوعين من الإرهاب السيبراني: أولهما هو الإرهاب السيبراني الخالص، وثانيهما هو الإرهاب السيبراني الخبيث.[30]

1) **الإرهاب السيبراني الخالص**: يتعلق بالهجمات المباشرة على البنية التحتية السيرانية للجهة المستهدفة من قبيل أجهزة الحاسوب، والشبكات، والمعلومات المخزنة فيهما، لتحقيق أهداف مختلفة. ويأخذ هذا النوع من الهجمات السيبرانية شكلين رئيسيين:

أ) **مهاجمة البيانات**: وهو الشكل الأكثر شيوعاً ويكون بمهاجمه البيانات بهدف سرقتها أو تدميرها مما يؤدى إلى عدم تقديم الخدمة التي كان يتم تقديمها من قبل.

---

[28] **د. رغدة البهي، "الإرهاب السيبراني: المفهوم والسمات والأنماط"، المركز المصري للفكر والدراسات الاستراتيجية، وحدة الإرهاب والصراعات المسلحة، 30 سبتمبر 2019، الرابط:**

https://www.ecsstudies.com/7141/

[29] **الموسوعة السياسية، مرجع سابق ذكره.**

[30] **د. رغدة البهي، "الإرهاب السيبراني: المفهوم والسمات والأنماط"، المركز المصري للفكر والدراسات الاستراتيجية، وحدة الإرهاب والصراعات المسلحة، 30 سبتمبر 2019، الرابط:**

https://www.ecsstudies.com/7141/

ب) **مهاجمة أنظمة التحكم:** ويترتب على ذلك تعطل البنية الأساسية المادية، كشبكة امدادات الطاقة، أو أمدادات المياه، أو السكك الحديدية أو غيرها. ومما لا شك فيه أن من شأن مثل هذا النوع من الهجمات إيقاع آثاراً كارثية تفوق تلك التي قد تنتج عن الإرهاب التقليدي في أقصي صوره.

2) **الإرهاب السيبراني الهجين:** وتحت هذا النوع تندرج الوظائف التقليدية للإرهاب من خلال استخدام شبكة الإنترنيت، سواء الدعاية والحرب النفسية، وتجنيد الأعضاء الجدد، والتواصل الآمن، وجمع التبرعات وغيرها من الأنشطة السالف الإشارة إليها.

ويتسم الأمن السيبراني بتعدد الأبعاد، فهناك البعد العسكري (الذي قد يأخذ شكل اختراق أنظمة الحماية الإليكترونية للمنشآت والآليات العسكرية بما في ذلك النووية منها) والبعد الاقتصادي (المتصل بالمصالح الاقتصادية للدول وشبكات معلومات البنوك بما فيها من تحويلات وقروض ومعاملات وعقود تجارية اليكترونية على مستوي العالم)، والبعد القانوني (الخاص بالأنشطة الخاصة بحفظ المستندات القانونية وقواعد بيانات الأحوال الشخصية والمواليد والوفيات وكل ما يتصل بالحكومة الإليكترونية)، وأخيراً، هناك البعد السياسي (والمتصل بالعمل على اختراق شبكات أجهزة الدولة الحساسة للحصول على معلومات سرية يتم الكشف عنها أمام الملايين من البشر في لحظة واحدة مما يعقد الأمور وقد يؤدى إلى إثارة القلاقل وعدم الاستقرار).[31]

المطلب الثاني: احتمالات صعود الإرهاب السيبراني

في واقع الأمر، عندما نتحدث عن الهجمات السيبرانية ذات الطابع العدائي فإننا لسنا في نطاق الخيال أو التصور؛ فعالمنا المعاصر أضحي بالفعل مسرحاً لتلك الهجمات السيبرانية التي يتم تقديمها، حتى الآن باعتبارها مجهولة المصدر، مع وجود إشارات إلى انتماء الكتائب التي تقوم بها إلى دول كبري. وفي هذا الخصوص نشير إلى بعض النماذج الحديثة لذلك:

---

[31] **د. علم الدين بانفا، مخاطر الهجمات الإليكترونية السيبرانية وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي، المعهد العربي للتخطيط، الكويت، سلسلة دراسات تنموية، 2019، الرابط:**
https://archive.org/details/20200616_20200616_2337/page/n3/mode/2up

- الاتهامات التي تم توجيهها إلى روسيا بالتدخل (اليكترونياً) في الانتخابات الأمريكية عام 2017 لضمان فوز المرشح الجمهوري آنذاك، كذلك تعرضت الولايات المتحدة لهجوم تضرر منه 50 شركة في ديسمبر 2020 كما أعلنت شركة الأمن السيبراني الأمريكية التي استطاعت تحديد الاختراق الواسع لوكالات حكومية أمريكية أن من بنيها وزارة الخزانة والأمن الداخلي والدفاع. وقد حمل آنذاك وزير الخارجية الأمريكي روسيا المسئولية عن الهجوم مثله مثل رؤساء لجان المخابرات في مجلسي الشيوخ والنواب.[32]

- اتهام دول غربية الصين بتنفيذ هجوم كبير وفي وقت سابق من العام الحالي استهدف خوادم شركة مايكروسوفت مما أثر على ما لا يقل عن 30 ألف مؤسسة على مستوى العالم. وعلى حين ذهبت التصريحات البريطانية في اتجاه أن جهات صينية مدعومة من الحكومة مسئولة عن الهجوم، صرح الاتحاد الأوروبي بان الهجوم "جاء من الأراضي الصينية".[33]

- تعرض الولايات المتحدة الأمريكية، خلال شهر يوليو 2021، لهجمة سيبيرانية خطيرة، هي الأولي في عهد الرئيس جوزيف بايدون، وكان لها تبعات كبيرة على العديد من الشركات والهيئات الأمريكية، وفي حين سارت التكهنات أن مصدر الهجمات جاء من الأراضي الروسية، فقد اكتفي الرئيس الأمريكي بالقول بأن من المنطقي بالنسبة لبلادة أن تشن هجمات على الخوادم المستخدمة في الهجمات السيبرانية على شركات ومؤسسات بلاده، مشيراً إلى أن الولايات المتحدة وجهت العديد من الطلبات إلى روسيا عبر القنوات الدبلوماسية لكي تتعامل مع الهجمات التي تقول واشنطن أنها تنطلق من الأراضي الروسية.[34]

وفيما يخص احتمالات تمكن التنظيمات الإرهابية التي تم تناولها في المبحث الأول من هذه الدراسة من الانخراط في مستوي الإرهاب السيبراني، فإن التنظيمات الجهادية التي تقدم نفسها على الإسلام الحقيقي وترفع شعار محاربة الكفار، هي المرشحة أكثر لدخول هذا المجال، حيث أنه ليس من مبرر معروف لدى جماعات اليمين المتطرف للقيام بذلك كما أنه ليس هناك هدف محدد يكمن استهدافه.

---

[32] https://www.bbc.com/arabic/science-and-tech-55383496

[33] https://www.bbc.com/arabic/science-and-tech-57893908

[34] https://arabic.rt.com/world/1250247

في المقابل فإن تنظيم "القاعدة" الذي بدأ ينشط مؤخراً، خاصة في أفغانستان، مع بدء انسحاب القوات الأمريكية والأوروبية التي كانت متمركزة فيها منذ فترة طويلة، وكذلك تنظيم "الدولة الإسلامية/داعش" الذي عاد للظهور بقوة في منطقة أفريقيا جنوب الصحراء، يمكنهما الانخراط في مثل هذه الأنشطة.

يساعد على ترجيح هذا الاحتمال المستوي المتفوق الذي سبق لتنظيم "الدول الإسلامية/داعش" الكشف عنه في استخدام شبكة الإنترنيت بمهارة، خاصة في جانبها المظلم لشراء السلاح والحصول على التمويل وتبادل المعلومات الاستخباراتة من خلال استخدام العملات الرقمية المشفرة، ومن جانب آخر، نجح التنظيم منذ منتصف العقد الماضي في تشكيل كتائب متخصصة تحت مسميات عديدة من بينها: "الخلافة الشبح" و "جيش أبناء الخلافة"، و"جيش الخلافة السيبراني"و "كلاشينكوف الأمن الإليكتروني"، وتجميعهم في اطار واحد تحت مسمي "الخلافة السيبرانية المتحدة".[35]

أما من الناحية العملية، فقد تم بالفعل تسجيل بعض الهجمات المنسوبة إلى هذا التنظيم ومنها:

- قيام مجموعة من القراصنة التابعين لتنظيم الدولة الإسلامية في تونس وتسمي The Fallaga بمهاجمة وتشويه عدد من المواقع الإليكترونية التابعة لوزارة الصحة البريطانية، تم من خلالها استبدال صفحات من الموقع بصور من ن طريق تغير صورة ملفها الشخصي بصور من الواقع السوري وكتابة رسائل من قبيل "أوقفوا القتل في سوريا" و "أنقذوا حلب من روسيا".
- قيام مجموعة من العناصر الإليكترونية التابعة للتنظيم باختراق حسابات الشرطة الماليزية الملكية على فيسبوك وتويتر عن طريق تغيير ملفها الشخص وصورة الغلاف.
- قيام قراصنة "الخلافة السيرانية المتحدة" بنشر مقطع فيديو تدعو فيه القراصنة المسلمين لتوظيف قدراتهم على الإختراق في مواجهة مختلف الدول.
- تمكن قراصنة "الخلافة السيرانية المتحدة" من اختراق مواقع الخطوط الجوية الماليزية والتحكم في موقع بث الإذاعة الفرنسية، ومحطات التلفزة الفرنسية وحساباتها على تويتر وفيسبوك.
- اختر ق حسابات القيادة المركزية العسكرية الأمريكية على اليوتيوب وتويتر، حيث تم استبدال شعار القيادة المركزية بصرة رجل ملثم مع ظهور كلمة Cyber Caliphate.[36]

[35] د. رغدة البهي، مرجع سابق.

[36] المرجع السابق.

في ضوء ما تقدم، يمكن القول بأنه ليس من المستبعد انخراط التنظمات الجهادية المتطرفة في هجمات سيرانية تحل محل الهجمات الإرهابية التقليدية أو تجري بالتوازي معها أو تمهيداً للقيامها في مناطق ذات طبيعة حساسة للغاية في الدول التي تناصبها العداء. ويتوقف الأمر بطبيعة الحال على مدي قدرة تنظيم "الدولة الإسلامية/داعش" على إعادة تنظيم صفوفه بطريقة مختلفة، ووضع خطط ذا طابع مختلف، وإقامة التحالفات مع التنظيمات الأخرى لتشكيل قوة تقنية متنوعة القدرات.

خاتمة

في الوقت الذي يركز فيه المؤتمر الدولي الأولي حول الأمن السيبراني في الدول العربية المنعقد في مراكش حول تجارب الدول العربية في هذا المجال بهدف تقييمها وطرح تصورات لسد ما قد يوجد بها من ثغرات، حرصت هذه الدراسة على طرح بعد أكثر شمولية وعمقاً ويتمثل في تناول المفهوم العكسي، ألا وهو "الإرهاب السيبراني". فإذا ما كانت هناك رغبة لتحقيق الأمن السيبراني من خلال تشريع القوانين وتحديد العقوبات، فإن هذا يعنى وجود توجه لمواجهة "الإرهاب السيبراني".

توصلت الدراسة إلى عدد من النتائج أبرزها ما يلي:

1) وجود خلط في المفاهيم في هذا المجال الجديد من مجالات الجريمة المنظمة بين الجرائم الإليكترونية، والجرائم السيبراينية، وامن المعلومات، والأمن السيبراني، وأخيراً الإرهاب السيبراني.

2) تظهر النظرة السريعة إلى التشريعات التي سنتها أغلب الدول العربية تركيزاً واضحاً على الجرائم الإليكترونية، فعلي سبيل المثال بالنظر إلى القانون المصري رقم (175) لسنة 2018 تحت مسمي "مكافحة جرائم تقنية المعلومات"، وقد تعامل القانون بشلك رئيسي مع الجرائم الإليكترونية من قبيل الاعتداء على حرمة الحياة الخاصة، أو اصطناع الحسابات والبريد الإليكتروني، أو جرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني، أو تدال أجهزة مطورة أو مشفرة. وخرجت المادة (21) من القانون عن هذا السياق للتحدث عن "جريمة الاعتداء على سلامة الشبكة المعلوماتية"، دون أن توضح المقصود بذلك على وجه التحديد، واقتصرت المادة على تحديد العقوبات

المفروضة في مثل هذه الحالات والتي تتمثل في الحبس لمدة ستة أشهر وبغرامة لا تقل عن مائة ألف جنية ولا تجاوز خمسمائة ألف جنية، أو بإحدى هاتين العقوبتين...".[37]

3) إبان الحرب ضد الإرهاب خلال النصف الثاني من العقد الماضي كانت التنظيمات الجهادية المتطرفة أكثر تقدماً من حيث الأسلوب من التحالف الدولي بقيادة الولايات المتحدة الأمريكية، على الأقل في مجال الاستخدام الواسع والماهر لشبكة الإنترنيت الأمر الذي مكنها من تنفيذ أكبر عملية تجنيد واسعة النطاق ومتعددة الأعراق في التاريخ الذين أطلق عليهم "المقاتلون الأجانب" وجمع الأموال والتدريب والتخطيط للعمليات وتنفيذها.

4) على الرغم من القضاء على آخر معاقل تنظيم "الدولة الإسلامية/داعش" وتصفية زعيمها، إلا أو الواقع يشير إلى أن التنظيم لم ينتهي، بل ظل قائماً يسعى إلى إعادة تنظيم صفوفه واستنساخ نفسه في صورة مختلفة، وقد ساعده على ذلك تداعيات تفشي جائحة كوفيد 19 التي أدت احتلت المستوى الأول في أولويات الدول في كافة أنحاء العالم، في وقت انشغلت فيه قوات الأمن بفرض التدابير الاحترازية ومواجهة المظاهرات المعارضة لهذه التدابير وتأمين الحدود وغيرها من المهام التي فرضتها ضرورة التعامل مع الموقف.

5) الحديث عن الهجمات السيرانية ليس خيالاً حيث جرت مثل هذه الهجمات خاصة فيما بين الدول الكبرى في سياق من تبادل الاتهامات والوعيد بالرد بالمثل.

6) أظهرت الخبرة الماضية امتلاك تنظيم "الدولة الإسلامية/داعش" القدرة الفنية على الانخراط في مجال الهجمات السيبرانية بما يعنيه ذلك من الحديث عن "الإرهاب السيراني" والذي تتجاوز خطورته بكثير الإرهاب التقليدي الذي عرفه العالم، منذ بداية القرن الحالي.

وفي النهاية يمكن طرح عدد من التوصيات نوجزها فيما يلي:

1. ضرورة المراجعة الدورية لقوانين الجرائم الإليكترونية التي أصدرتها الدول العربية وتحديثها لتشمل طائفة أوسع من الجرائم بما في ذلك الإرهاب السيبراني.

---

[37] **القانون رقم (175) لسنة 2018، الرابط**

http://laweg.net/Default.aspx?action=ViewActivePages&ItemID=112278&Type=6

2. قد يكون من المفيد وضع قانون مشترك حول "الإرهاب السيبراني" في إطار جامعة الدول العربية.

3. أهمية تشكيل كتائب اليكترونية على درجة عالية من الكفاءة من مختلف الدول العربية يمكنها البحث في وضع نظام أمن سيبراني يحتوي على مستويات متعددة من الأمان يصعب اختراقها في صمت دون إطلاق أجهزة إنذار تمكن من التعامل الفوري مع الموقف وتجنب وقوع الخسائر.

4. ضرورة التنسيق مع معهد الأمم المتحدة الأقاليمي لأبحاث الجريمة والعدالة، التابع للمجلس الاقتصادي والاجتماعي للأمم المتحدة، على تنظيم مؤتمر دولي لتقديم عرض شامل لنتائج دراساته حول موضوع الإمن والإرهاب السيبراني، في ضوء المشروع الذي دشنه عام 2014 تحت مسمي "برنامج البحوث الأوروبي بشأن الجريمة السيبرانيه والإرهاب السيبراني، للاستفادة منها في الوقت المناسب.

5. المتابعة الدورية لنظم تأمين الشبكات والأنظمة ووضع نظم إنذار على درجة عالية من الكفاءة، بشرط أن تكون مصنوعة على يد نخبة من الخبراء المحليين، للكشف عن أي محاولة اختراق.

6. العمل على تأمين نظم التواصل عن بعد والتي يتم استخدامها حالياً في التعليم وأداء الوظائف الحكومية واللقاءات والندوات بشكل يحول دون اختراقها وتغيير مضمونها لأهداف إرهابية.

قائمة المراجع

أولاً- الكتب باللغة العربية:

1. د. أحمد أبو الروس، الإرهاب والتطرف والعنف الدولي، المكتب الجامعية الحديث، الإسكندرية، مصر، 2001.
2. د. داليا مجدي عبد الغنى، أيدولوجية الإرهاب وآليات مكافحته وفقاً لأحدث التشريعات والاتفاقيات الدولية القاهرة، دار النهضة العربية، الإمارات، دار النهضة العلمية، 2018.
3. د. عماد عواد، المواطنة والأمن، تقديم د. بطرس بطرس غالي، القاهرة، دار النهضة العربية، مصر، 2010.
4. د. عماد عواد، الإرهاب واستراتيجية المتعامل، دار النهضة العربية، القاهرة، مصر، 2019.
5. د. عماد عواد، ليندا عواد، كوفيد 19 وحقوق الإنسان، تقديم الوزير/ محمد فايق: رئيس المجلس الوطني لحقوق الإنسان، دار النهضة العربية، القاهرة، مصر، 2021.

ثانياً- الكتب والتقارير الأجنبية

- Jean-Paul Marthoz, Terrorism and the Media: a handbook for Journalists, UNESCO, Paris, France, 2017.
https://unesdoc.unesco.org/ark:/48223/pf0000247074
- Shadi Hamid, "The Roots of the Islamic State's Appeal", Brookings Institute, 31 October 2014.
https://www.brookings.edu/opinions/the-roots-of-the-islamic-states-appeal/
- Beyond the Caliphate: Foreign Fighters and the Threat of Returnees, The SOUFAN Center, October 2017.

ثالثاً- مصادر على شبكة الإنترنيت

- http://thesoufancenter.org/wp-content/uploads/2017/11/Beyond-the-Caliphate-Foreign-Fighters-and-the-Threat-of-Returnees-TSC-Report-October-2017-v3.pdf

رابعاً مقالات وأبحاث

1. د. رغدة البهي، "الإرهاب السيبراني: المفهوم والسمات والأنماط"، المركز المصري للفكر والدراسات الاستراتيجية، وحدة الإرهاب والصراعات المسلحة، 30 سبتمبر 2019، الرابط:
   - https://www.ecsstudies.com/7141/
2. شاكر نوري، "الإرهاب في الإعلام الفرنسي... من الصورة النمطية إلى الصورة الانفجارية"، (موقع نزوة: 17 يناير 2018)، تاريخ الاطلاع 28 نوفمبر 2018.
   - https://www.nizwa.com/الإرهاب-في-الإعلام-الفرنسي-من-الصورة/
3. عامر دكة، "النازيون الجدد يطلون بروؤسهم في الولايات المتحدة"، (موقع المصدر: 23 نوفمبر 2016) تاريخ الاطلاع 29 نوفمبر 2018.
   - https://www.al-masdar.net/النازيون-الجدد-يطلون-بروؤسهم-في-الولا

4. د. علم الدين بانقا، مخاطر الهجمات الإليكترونية السيبرانية وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي، المعهد العربي للتخطيط، الكويت، سلسلة دراسات تنموية، 2019، الرابط:

- https://archive.org/details/20200616_20200616_2337/page/n3/mode/2up

5. محمد الحمامصي، "الانترنيت شرك في صناعة الإرهاب في العالم"، (لندن: موقع جريدة العرب، 2015/2/2). تاريخ الاطلاع 29 نوفمبر 2018.

- https://alarab.co.uk/الإنترنت-شريك-صناعة-الإرهاب-في-العالم

خامساً- مستندات الأمم المتحدة

(1) تقرير الأمين العام للأمم المتحدة عن التهديد الذي يشكله تنظيم الدولة الإسلامية في العراق والشام (تنظيم داعش) على السلام والأمن الدوليين، ونطاق الجهود التي تبذلها الأمم المتحدة دعماً للدول الأعضاء في مكافحة هذا التهديد، 29 كانون الثاني/يناير 2016. موقع الأمم المتحدة.

- http://undocs.org/ar/S/2016/92
- https://www.unodc.org/

سادساً- مراجع أخري

1 الموسوعة السياسية، الرابط

- https://political-encyclopedia.org/

الأمن السيبراني في القوانين والاستراتيجيات والسياسات الوطنية في المملكة الأردنية الهاشمية دراسة تحليلية

الأستاذ محمد أحمد الجراح

باحث وخبير في مجال الأمن السيبراني (الأردن)

الملخص:

في السنوات القليلة الماضية قامت العديد من الدول العربية بنشر قوانين وتشريعات واستراتيجيات وطنية في مجال الأمن السيبراني وتم تسميتها بهذا الاسم وكانت المملكة الأردنية الهاشمية إحدى هذه الدول حيث قامت بإنشاء ونشر القوانين والتشريعات والاستراتيجيات المتعلقة بالأمن السيبراني، تم نشر قانون الأمن السيبراني رقم (16) لسنة 2019 بتاريخ 16-9-2019 بالجريدة الرسمية والذي نص على إنشاء مجلس يسمى المجلس الوطني للأمن السيبراني وكذلك مركز يسمى المركز الوطني للأمن السيبراني وذكر المهام الموكلة لكل منهما حيث تكونت الوثيقة الخاصة بهذا القانون من (11) صفحة و (19) مادة.

انتهت المدة المحددة للاستراتيجية الوطنية لضمان أمن المعلومات والأمن السيبراني 2012 في عام 2017 وتم تجهيز الإستراتيجية الوطنية للأمن السيبراني للأعوام (2018-2023) والتي كان الهدف منها تحديد الأدوار المنوطة بالحكومة الأردنية لتحقيق الرؤية الخاصة بحماية الأصول المعلوماتية وبالتنسيق مع القيادة العامة للقوات المسلحة الأردنية الجيش العربي، وبمساعدة الشركة البريطانية British Aerospace Systems (BAE) وهي شركة عالمية متخصصة بالأمن السيبراني ونشرت باللغتين العربية والإنجليزية معا وكان مجموع صفحاتها (29) صفحة وغطت هذه الاستراتيجية أربعة محاور رئيسية هي الحماية والاستكشاف والاستجابة والتطور وتم انشاؤها من قبل الحكومة التزاما بنص المادة (142) من السياسة العامة للحكومة في قطاعات الاتصالات وتكنولوجيا المعلومات والبريد لعام 2012 وانبثق عن هذه الاستراتيجية البرنامج الوطني للأمن السيبراني والذي تم فيه انشاء (20) وثيقة ضمت سياسات وأطر الأمن السيبراني ضمن ستة أقسام وبما مجموعة (241) صفحة تم بيان أهم ما جاء فيها ضمن هذه الورقة.

ومع الانفتاح في الدولة الأردنية في مجال الأمن السيبراني أصبح هنالك العديد من المؤتمرات والندوات حول الموضوع وكذلك قامت العديد من الجامعات الحكومية والخاصة بفتح تخصص الأمن السيبراني وتم انشاء العديد من

المختبرات الخاصة بالأمن السيبراني في الجامعات وبعض الشركات وتم تشجيع الطلاب والدارسين للدخول في هذا المجال وبيان أهميته ومدى افتقار سوق العمل لهذا المجال ومدى قدرته على استيعاب الوظائف التي تتعلق بهذا التخصص.

خلصت هذه الورقة إلى تحليل وبيان القوانين والاستراتيجيات والسياسات المنشورة في المملكة الأردنية الهاشمية بما يخص الأمن السيبراني وإبراز الإيجابيات والتطلعات المستقبلية والمآخذ المتعلقة بها.

Abstract

In the past few years, many Arab countries have published national laws, legislation, and strategies in the field of cybersecurity and were named by this name, the Hashemite Kingdom of Jordan was one of these countries, where it created and published laws, legislation and strategies related to cybersecurity, the Cyber Security Law No. 16 of the year 2019 has published in the Official Gazette on 16-09-2019, which talked about establishment of a council called the National Cyber Security Council, as well as a center called the National Cyber Security Center, and mentioned the tasks assigned to each of them, as the document for this law consisted of (11) pages and (19) articles.

The period specified for the National Information Assurance and Cyber Security Strategy 2012 expired in 2017, and the National Cybersecurity Strategy for the years (2018-2023) was prepared, which aimed at defining the roles assigned to the Jordanian government to achieve the vision of protecting information assets and in coordination with the General Command of the Jordanian Armed Forces, With the help of the British company British Aerospace Systems (BAE) global company specializing in cyber security, and published in both Arabic and English languages, its pages totaled (29) pages. This strategy covered four main hubs: protection, exploration, response and development, and it was established by the government in compliance with the text of Article (142) of the General Policy for the Information & Communications Technology and Postal Sectors for the year 2012. From this strategy emerged the National Program for Cyber Security, in which (20) documents were created that included cybersecurity policies and frameworks within six sections, with a total of (241) pages, the most important of which were stated within this paper.

With the openness in Jordan on the field of cybersecurity, there have been many conferences and seminars on this subject, as well as many public and private universities have opened specific major of cybersecurity, and many cybersecurity laboratories have been established in universities also in many companies. Students and scholars were encouraged to enter this field and to indicate its importance and the extent to which the labor market absorbs and lacks jobs related to this major.

This paper concludes by analyzing and clarifying the laws, strategies and policies published in the Hashemite Kingdom of Jordan about cybersecurity and highlighting the positives, future aspirations and drawbacks related to them.

المقدمة

انتشر مصطلح الأمن السيبراني بشكل واسع في السنوات الماضية وأصبحت العديد من الدول تنشر القوانين والسياسات والأنظمة بهذا الاسم وكلمة سيبراني هي تعريب للكلمة الإنجليزية (Cyber) والتي تعني في المترجمات (الإلكترونية) والتي أصبحت تدل على كل ما يتعلق بالاتصالات وتقنية المعلومات، والتي تم اشتقاقها من كلمة (Cybernetics) السيبرنتيكا والتي تعرف بالعربية بعلم الضبط أو بعلم التحكم الذاتي او علم التربين وتعني الحكم أو التوجيه والإدارة (التربين) [38] ومنها الرُّبَّان وهو علم حديث نوعيا ظهر في بداية الأربعينيات من القرن العشرين ويعتبر الرياضي نوربرت فينر من أهم مؤسسيه وقد عرف فينر السِبرانية على أنها "علم القيادة أو التحكم في الأحياء والآلات ودراسة آليات التواصل في كل منهما. (1) (2) [39]

وفي القرن الحادي والعشرين، أُستُخدم هذا المصطلح بطريقة واسعة بما يخص أنظمة الاتصالات وتقنية المعلومات وطريقة التواصل فيما بينها وعليه أصبح يوجد كلمات مثل مقهى إنترنت (Cybercafé) وهي المحلات التجارية التي تقدم خدمة الإنترنت وأيضا مصطلح الجرائم الإلكترونية أو السيبرانية (Cybercrimes) ويقصد بها الجرائم التي تحصل عن طريق الإنترنت والحواسيب وكذلك ظهر مصطلح الأمن السيبراني (Cybersecurity).

وعرف القانون الأردني للأمن السيبراني قانــون رقم (16) لسنة 2019 الأمن السيبرانـي على أنه الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني والقدرة على استعادة عملها واستمراريتها سواء أكان الوصول إليها بدون تصريح أو سوء استخدام او نتيجة الاخفاق في اتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي لذلك. (3) [40]

---

[38] : صليبا، جميل المعجم الفلسفي الجزء الأول صفحة 682

[39] البعلبكي، منير موسوعة المورد صفحة 307 السِّيبرَناتية؛ علم الضبط

[40] المملكة الأردنية الهاشمية، رئاسة الوزراء، الجريدة الرسمية عدد 5595، قانــون رقم (16) لسنة 2019 - قانون الأمن السيبرانـي

كان يتعارف على مصطلح الأمن السيبراني بأمن المعلومات إلا أنه ومع وجود فوارق بينهما خصوصا أن أمن المعلومات يشمل أمن المعلومات على الوثائق الورقية والمطبوعات وأن الأمن السيبراني يشمل على حفظ وجود الاتصالات وشبكات الاتصال أصبح العديد من الناس يفرق بينهم في الاستخدام ويدعو بشكل واسع إلى نشر مصطلح الأمن السيبراني مع العلم أنه برأي الباحث أن مصطلح أمن أنظمة الاتصالات وتقنية المعلومات يدل على مصطلح الأمن السيبراني لكن باستخدام مفردات عربية.

ومع هذا الاستخدام الواسع للمصطلح واعتماد الكثير من الدول والحكومات و المؤسسات العامة والخاصة والأفراد في تعاملاتهم واستثماراتهم وتواصلهم فيما بينهم على الانترنت وتقنية الاتصال وأنظمة المعلومات واعتمادهم على طرق تقنية المعلومات لحفظ البيانات خصوصا الحساسة منها وللشراء والاستثمار وعرض المنتجات لدرجة أنها أصبحت تدخل في غالبية شؤون الحياة وتديرها أصبحت الدول العالمية تقوم بإنشاء قوانين وتشريعات وصياغة استراتيجيات وسياسات بخصوص الأمن السيبراني وقامت العديد من الدول العربية بمثل ذلك مثل الأردن والمغرب والسعودية والإمارات ومصر وغيرها.

لمحة تاريخية عن الاستراتيجيات المتعلقة بالأمن السيبراني في المملكة الأردنية الهاشمية

قامت المملكة الأردنية الهاشمية بإنشاء العديد من الاستراتيجيات الخاصة بالأمن السيبراني ومنذ مدة طويلة وكانت من الدول السباقة في المنطقة بهذا المجال حيث قام مجلس الوزراء الأردني في العام 2007 بإقرار وثيقة السياسة العامة للحكومة في قطاعات الاتصالات وتكنولوجيا المعلومات والبريد 2007 والتي تضمنت أكثر من مادة تتحدث عن أمن المعلومات وتشكيل وحدة فنية متخصصة بأمن وحماية المعلومات (سيرت في الأردن)[41] [(1)] وتبعها في العام 2008 إعداد السياسات الوطنية لأمن المعلومات والتي اقرت ونشرت من قبل وزارة الاتصالات وتكنولوجيا المعلومات بعد اعتمادها من رئاسة الوزراء بتاريخ 28-10-2008 وتم إعدادها من قبل اللجنة الوطنية لأمن وحماية المعلومات وكانت ضمن وثيقة واحدة تكونت من (57) صفحة باللغة العربية[42] [(2)] وتحدثت عن العديد من الأمور المتعلقة بأمن وحماية المعلومات والأمن السيبراني الذي لم يكن يطلق عليه هذا الاسم في الأردن في ذلك الوقت وكانت هذه السياسة شاملة ومتكاملة واحتوت على مجموعة من التعريفات الخاصة بهذا المجال وتحديد الأدوار والمسؤوليات واشتملت على مجموعة من السياسات الوطنية لأمن وحماية المعلومات

[41] المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "السياسة العامة للحكومة في قطاعات الاتصالات وتكنولوجيا المعلومات والبريد 2007".

[42] المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "السياسات الوطنية لأمن وحماية المعلومات" 2008.

كان عددها (17) سياسة وهي : سياسة حساسية وتصنيف المعلومات وسياسة الاستعمال المقبول وسياسة ضبط التغيير وميثاق السلوك الخاص بأمن المعلومات وسياسة التدقيق الخاص بأمن المعلومات وسياسة الأمن المادي وسياسة أمن الموظفين وسياسة الحاسوب المكتبي وسياسة الأجهزة المحمولة وسياسة كلمات المرور وسياسة مكافحة الفيروسات والبرامج الخبيثة وسياسة البريد الإلكتروني وسياسة النسخ الاحتياطي وسياسة أمن الشبكات وسياسة تطوير وصيانة الأنظمة وسياسة التعاقد الخارجي وسياسة التشفير ولم يتم تحديد مدة زمنية لانتهاء هذه السياسة.

وقام مجلس الوزراء الأردني في العام 2012 بإقرار الاستراتيجية الوطنية لضمان امن المعلومات وامن الفضاء السيبراني 2012 – 2017[43] [(3)] والتي تم اعدادها من قبل وزارة الاتصالات وتكنولوجيا المعلومات وجاءت هذه الإستراتيجية استجابة للتهديدات التي تفرضها التغيرات الهائلة والسريعة في تكنولوجيا المعلومات والاتصالات. وتهدف الى تعزيز الأمن الوطني الأردني من خلال منع الهجمات الإلكترونية وتقليل المخاطر على البنى التحتية الحيوية الحرجة وبالتالي تعزيز الاقتصاد الاردني عن طريق زيادة الثقة بأنظمة المعلومات الحكومية والخاصة. وقامت وزارة الاتصالات وتكنولوجيا المعلومات الأردنية بالتعاون مع مركز تكنولوجيا المعلومات الوطني بإعداد الخطة التنفيذية لإنشاء فريق "سيرت الأردن" وكذلك تحدثت عن بناء القدرات والتدريب في هذا المجال وتطوير معايير وسياسات خاصة بالأمن السيبراني في الأردن ونظام التشفير الوطني وكذلك أمن

وحماية المعلومات والشبكات والذي تضمن أكثر من بند مثل الحماية الشخصية والأمن المادي وحماية الشبكات والاتصال وأمن البرمجيات وإجراءات الحماية المتعلقة أمن الانبعاثات الكهرومغناطيسية (الإشعاعات) وكذلك برنامج حماية البنية التحتية الوطنية الحرجة أو الحساسة ووضع خارطة طريق من اجل تطبيق هذه السياسة.

بعد إقرار الاستراتيجية الوطنية لضمان امن المعلومات وامن الفضاء السيبراني 2012 تم إقرار السياسة العامة للحكومة في قطاعات الاتصالات وتكنولوجيا المعلومات والبريد2012 والتي تكونت من (72) صفحة و(188) مادة باللغتين العربية والإنجليزية واحتوت على فصل كامل يتعلق بقطاع تكنولوجيا المعلومات والذي

[43] **المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "الاستراتيجية الوطنية لضمان امن المعلومات وامن الفضاء السيبراني 2012**

احتوى على فرع تكون من أربعة مواد خاص بحماية الملكية الفكرية والاستخدام الأمن للإنترنت وكذلك احتوى على فرع تكون من أربعة مواد خاص بالمحافظة على أمن تكنولوجيا المعلومات[44] (1).

خلفا للاستراتيجية الوطنية لضمان أمن المعلومات والأمن السيبراني 2012 والتي انتهت في العام 2017 قامت وزارة الاتصالات وتكنولوجيا المعلومات الأردنية تجهيز ونشر الاستراتيجية الوطنية للأمن السيبراني للأعوام (2018-2023)[45](2) وتم ذلك بالتنسيق مع القيادة العامة للقوات المسلحة الأردنية الجيش العربي، وبمساعدة احدى الشركات البريطانية ونشرت باللغتين العربية والإنجليزية وكان مجموع صفحاتها (29) صفحة وغطت هذه الاستراتيجية أربعة محاور رئيسية هي الحماية والاستكشاف والاستجابة والتطور وبعد الانتهاء منها تم صياغة ونشر السياسات والأطر الوطنية للأمن السيبراني من قبل وزارة الاتصالات وتكنولوجيا المعلومات الأردنية وبالتعاون مع القوات المسلحة الأردنية والذي تكون من (20) وثيقة وتم ربط جميع هذه الوثائق بالإستراتيجية الوطنية للأمن السيبراني.

في العام 2018 تم تحديث السياسة العامة لقطاعات الاتصالات وتكنولوجيا المعلومات والبريد وإقرار السياسة الجديدة من قبل وزارة الاتصالات تكنولوجيا المعلومات ونشر السياسة الجديدة والتي تكونت من (33) صفحة و (151) مادة باللغتين العربية والإنجليزية[46] (3) وحيث وجهت هذه السياسة كافة المواد والإجراءات المتعلقة بالأمن السيبراني إلى الاستراتيجية الوطنية للأمن السيبراني (2018-2023) وتم ذكر ذلك في كل من المادة رقم (90) والمادة رقم (148) وبذلك تم ربط كافة الوثائق المتعلقة بالأمن السيبراني بالإستراتيجية الوطنية للأمن السيبراني.

قانون الأمن السيبراني الأردني

قامت المملكة الأردنية الهاشمية بإقرار قانــون رقم (16) لسنة 2019 - قانون الأمن السيبرانـي بتاريخ 16-9-2019 في العدد رقم 5595 من الجريدة الرسمية[47] (4) ولكن جاء هذا القانون بمخالفة نص قانون أخر تم اقراره

---

[44] المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "وثيقة السياسة العامة للحكومة في قطاعات الاتصالات وتكنولوجيا المعلومات والبريد للعام،" 2012.

[45] المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "الاستراتيجية الوطنية للأمن_السيبراني 2018 - 2023", 2018

[46] المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "السياسة العامة لقطاعات الاتصالات وتكنولوجيا المعلومات والبريد 2018".

[47] المملكة الأردنية الهاشمية، رئاسة الوزراء، الجريدة الرسمية عدد 5595، قانــون رقم (16) لسنة 2019 - قانون الأمن السيبرانـي.

سابقا حيث نصت المادة (11) من قانون حماية اللغة العربية رقم 35 لعام 2015 "تصاغ جميع تشريعات الدولة باللغة العربية"[48] (5) وبما أن لقوانين الأردنية المنشورة سابقا، ولكن ذلك لم يمنع من إقراره ونشره مع العلم أنه برأي الباحث انه كان من الممكن تسميته بقانون أمن أنظمة الاتصالات وتقنية المعلومات، وكان القانون الأول من نوعه حيث كانت القوانين السابقة تعنى بالجرائم الإلكترونية فقط وتكون هذا القانون من (11) صفحة تضمنت (19) مادة.

بدأ قانون الأمن السيبراني الأردني بالتعريف بهذا القانون وتعريف المصطلحات والكلمات الدلالية فيه والتي كان عددها (12) مثل الأمن السيبراني والفضاء السيبراني والحادث السيبراني وغيرها، وانتقل بعدها إلى التحدث عن تشكيل مجلس يسمى (المجلس الوطني للأمن السيبراني) وطريقة اختيار أعضاء هذا المجلس ومما يجب أن يتكون وكيفية انعقاده، ثم ذكر مهام وصلاحيات المجلس. بعد ذلك تطرق القانون إلى ذكر تشكيل مركز مختص يتبع لرئيس الوزراء مباشرة ويسمى (المركز الوطني للأمن السيبراني) وتم بيان الهدف الذي تم إنشاؤه من أجله والمهام والصلاحيات الممنوحة له ومن ثم تطرق القانون إلى آلية تعيين رئيس المركز وكما أن القانون ذكر صراحة أن هذا المركز يعمل مع دائرة المخابرات العامة عند إعداد الاستراتيجيات والسياسات وبناء الأنظمة وشراء الخدمات اللازمة لأداء مهامه. وبعد ذلك تطرق القانون إلى تحديد حادث الأمن السيبراني الذي يشكل تهديدا وإلزام كافة الجهات بالالتزام بتعليمات وتوجيهات المركز. ومن ثم تطرق القانون إلى الحصول على تراخيص للعمل في مجال الأمن السيبراني. ومن أهم البنود والصلاحيات التي ذكرها القانون أنه يتم إعطاء صفة الضابطة العدلية لرئيس المركز والموظفين الذين يحددهم ويحق لهم دخول وتفتيش أي مكان تشير الدلائل لوجود ممارسات تخرق الأمن السيبراني ولهم الحق بضبط الأجهزة والوسائل والأدوات والبرامج وأنظمة المعلومات والشبكة المعلوماتية وتنظيم ضبط بحق المخالفين. وتطرف القانون إلى الموارد المالية الخاصة بالمركز والإجراءات التي من الممكن اتخاذها من قبل المركز للمخالفين. وتم تحديد نظام الخدمة في المركز وإمكانية إلحاق الموظفين فيه[49] (1). ومما سبق ذكره حول القانون يتبين بأنه قانون تنظيمي وليس قانونا تجريميا.

---

[48] المملكة الأردنية الهاشمية، رئاسة الوزراء، قانون رقم (35) لسنة 2015- قانون حماية اللغة العربية.

[49] المملكة الأردنية الهاشمية، رئاسة الوزراء، الجريدة الرسمية عدد 5595، قانون رقم (16) لسنة 2019 - قانون الأمن السيبراني

تبعا لقانون الأمن السيبراني وبمقتضى الفقرة (ج) من المادة السابعة منه تم إقرار نظام المركز الوطني للأمن السيبراني في الجريدة الرسمية في العدد رقم (5614) بتاريخ 2-1-2021[50] (2) والذي تكون من ثلاث صفحات وسبع مواد حيث بين أهم واجبات ومسؤوليات وصلاحيات المجلي ورئيس المجلس. وبتاريخ 1-6-2021 وفي العدد رقم 5721 من الجريدة الرسمية تم إقرار نظام التنظيم الإداري للمركز الوطني للأمن السيبراني[51] (3) والذي تكون من أربع صفحات وسبع مواد والتي وضحت الهيكل التنظيمي للمركز والإدارات التابعة له والمديريات التابعة لكل إدارة واللجان التابعة للمركز وارتباطاتها التنظيمية.

الاستراتيجيات والسياسات الوطنية للأمن السيبراني الحالية

الإستراتيجية الوطنية للأمن السيبراني 2018-2023

التزاما بنص المادة (142) من السياسة العامة للحكومة في قطاعات الاتصالات وتكنولوجيا المعلومات والبريد[52] 2012 (1) وخلفا للاستراتيجية الوطنية لضمان أمن المعلومات والأمن السيبراني 2012 والتي انتهت في العام 2017 تم تجهيز الاستراتيجية الوطنية للأمن السيبراني للأعوام (2018-2023)[53] (2) والتي يتم العمل بها حاليا والتي كان الهدف منها تحديد الأدوار المنوطة بالحكومة الأردنية لتحقيق الرؤية الخاصة بحماية الأصول المعلوماتية وبالتنسيق مع القيادة العامة للقوات المسلحة الأردنية الجيش العربي، وبمساعدة الشركة البريطانية British Aerospace Systems (BAE) ونشرت باللغتين العربية والإنجليزية وكان مجموع صفحاتها (29) صفحة وركزت هذه الإستراتيجية على أربعة محاور رئيسية هي الحماية والاستكشاف والاستجابة والتطور، وكذلك قامت بتحديد الأفعال التي يجب اتخاذها ضمن كل محور لتنفيذ هذه الإستراتيجية وتطبيقها وتحقيق الأهداف المرجوة منها على المستوى الوطني وبما يشمل الحكومة والمؤسسات العامة والخاصة والأفراد والبنى التحتية وخصوصا الحرجة منها كشبكات الكهرباء والاتصالات وكان من أهم أهداف هذه الإستراتيجية زيادة الموثوقية بتوفير البيئة الرقية الآمنة مما ينعكس ايجابا على تحفيز الاستثمار الحالي خصوصا مع التوجهات العالمية والمحلية بالتحول الرقمي ورقمنة القطاعات العامة والخاصة والاستثمارات مما يؤدي إلى استقطاب استثمارات جديدة وبالتالي تنمية الاقتصاد الوطني.

---

[50] المملكة الأردنية الهاشمية، رئاسة الوزراء، نظام رقم (1) لسنة 2020 -نظام المركز الوطني للأمن السيبراني

[51] المملكة الأردنية الهاشمية، رئاسة الوزراء، نظام رقم (25) لسنة 2021 - نظام التنظيم الإداري للمركز الوطني للأمن السيبراني

[52] المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "وثيقة السياسة العامة للحكومة في قطاعات الاتصالات وتكنولوجيا المعلومات والبريد للعام 2012".

[53] المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "الاستراتيجية الوطنية للأم_السيبراني 2018 - 2023

تحدثت هذه السياسة عن العديد من الأمور حيث ابتدأت بالتمهيد ومقدمة عن الأمن السيبراني وأهميته وبينت التقدم المحرز في تحقيق اهداف الاستراتيجية السابقة للأعوام (2012 – 2017) وتحدثت عن البرنامج الوطني للأمن السيبراني وأهم الإنجازات التي قدمها مثل تقييم مخاطر الشبكات الحرجة واستغلال مخرجات هذا التقييم لوضع معايير أمن المعلومات والسياسات اللازمة وانشاء فرق وطنية لحوادث الأمن السيبراني وتنفيذ برنامج تدريبي لتعزيز مهارات الجهات المعنية وانشاء برنامج للتعاون الدولي في هذا المجال وتم ذكر بعض التحديات التي واجهها البرنامج مثل الضرورة لوضع إطار قانوني وتنظيمي ملائم . وتطرقت هذه السياسة إلى واقع التهديدات المتنامية وذكرت مجموعة من الحوادث بهذا الخصوص وكما ذكرت مجموعة من جهات التهديد وأهم تحديات الأمن السيبراني خصوصا لتنوع أسباب الهجمات السيبرانية مثل الدافع المالي والدوافع السياسية والايدولوجية وبعض الطرق المستخدمة في ذلك وبعض نقاط الضعف في مجال الأمن السيبراني. ومن ثم تحدثت السياسة عن السياق الاستراتيجي والذي انقسم إلى رؤية الأمن السيبراني، والأهداف الاستراتيجية مثل الحماية والكشف والتحري والاستجابة والتطور، والمبادئ التوجيهية. وبعد ذلك تحدثت الاستراتيجية عن أولويات الأمن السيبراني الوطني والتي تضمنت معايير وسياسات الأمن السيبراني الوطني وبرنامج التعاون الدولي لأمن المعلومات وبرنامج التوعية بالأمن بناء القدرات وبرنامج حماية البنية التحتية الوطنية الحساسة والفرق الوطنية للاستجابة لحوادث الأمن السيبراني والإصلاح التنظيمي والقانوني. ومن ثم انتقلت إلى آلية تنفيذ الاستراتيجية والتي انقسمت إلى خطة التنفيذ وبما في ذلك من عمليات تحديد المسؤولية والتنسيق والتخطيط للتنفيذ، وإمكانيات الأمن السيبراني الوطني والهيئة الوطنية للأمن السيبراني وذكر أهم

المسؤوليات لهذه الهيئة وكذلك الأولويات الملحة لها مثل القيادة والحوكمة والتعاون الدولي واشراك القطاعات والتعليم والتدريب وبيان خطة العمل لكل من هذه الأولويات. ومن ثم تحدثت الاستراتيجية عن أهم المعالم لغاية العام 2023 وقسمت إلى المعالم الرئيسية وقياس مدى النجاح في تحقيق الأهداف الاستراتيجية الوطنية للأمن السيبراني واختتمت الاستراتيجية بالاستنتاجات وملحق قاموس المصطلحات والاختصارات.

ذكر في الاستراتيجية انه سيتم انشاء هيئة مستقلة للأمن السيبراني إلا أنه لم يتم انشاء هذه الهيئة وانما تم انشاء المجلس الوطني للأمن السيبراني والمركز الوطني للأمن السيبراني وكما سيتم بيانه في البنود اللاحقة المتعلقة بقانون الأمن السيبراني.

البرنامج الوطني وسياسات وأطر الأمن السيبراني

انبثق من الإستراتيجية الوطنية للأمن السيبراني انشاء برنامج وطني من أجل إعداد مجموعة من السياسات والأطر المتعلقة بالأمن السيبراني والتي وتم اعدادها ونشرها من قبل وزارة الاتصالات وتكنولوجيا المعلومات بالتعاون مع القوات المسلحة الأردنية وانقسمت إلى ست مجالات احتوت على (20) وثيقة مقسمة كما يلي:

المجال الأساسي 1: الحوكمة وإدارة المخاطر والامتثال والذي تكون من 4 وثائق وهي:

أ- الأدوار والمسائلة والمسؤوليات ، من المسؤول عن فعل ماذا ومن المسؤول عن من (1):[54] وتكونت هذه الوثيقة من (17) صفحة و (6) محاور تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها وثيقة ليست مستقلة دون باقي السياسات وبيان المتطلبات الأساسية للأدوار والمسائلة والمسؤوليات وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية وتطرقت إلى المعايير الدولية التي تمت الاستعانة بها مثل (ISO/IEC 27001) و (ISO/IEC 22301) و (ISO 9001) كما وتطرقت في محورها الثاني إلى مبادئ أمن المعلومات مثل السرية و سلامة المعلومات والتوفر وتطرقت إلى فهم كيفية التعامل مع أصول المعلومات و تدابير حماية أصول المعلومات وحماية سرية وسلامة وتوفر أصول المعلومات، ومن ثم تطرقت الوثيقة إلى مستوى الدخول إلى مبادئ السرية والسلامة والتوفر والتحرك حولها، والذي انقسم إلى مستوى الدخول إلى التطبيقات ومستوى الدخول إلى البنية التحتية ومستوى الدخول المادي ومستوى حركة البيانات وبعد ذلك جاء محورها الثالث والذي يعنى بالاستجابة الوطنية المنسقة والذي تحدث عن التنظيم الخاص بالأمن السيبراني لدى كافة العاملين والامتثال للمتطلبات والمعايير العالمية والهيكل التنظيمي والمكونات الوطنية والذي تضمن الاستراتيجية الوطنية للأمن السيبراني والبرنامج الوطني للأمن السيبراني والوكالة الوطنية/ المركز الوطني للأمن السيبراني واحتوى المحور الرابع "مبدأ وطني للامتثال والمحور الخامس " الأدوار والمسؤوليات والذي تضمن تحديد الأدوار والتعريف بالأدوار والمسؤوليات الخاصة بالعديد من الجهات والعديد من المناصب في الدولة الأردنية ومن ثم الإيجاز والتوضيح حول الأدوار والمسؤوليات وبعد ذلك تحدثت عن المسائلة وجاء المحور

[54] المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 1 (أ) الأدوار والمسائلة والمسؤوليات.

السادس ليتحدث عن " الإبلاغ عن حادث" والذي تضمن إبلاغ إدارة تكنولوجيا المعلومات عن انتهاكات أو اختراقات للأمن أو للسياسة وتم إلحاق جدول (RASCI) المختص بتحديد الأدوار والمسؤوليات.

(ب): إدارة المخاطر، كيفية تقييم وتقدير المخاطر وإدارتها (1) :[55] وتكونت هذه الوثيقة من (15) صفحة و (5) محاور تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها وثيقة ليست مستقلة دون باقي السياسات، وبيان المتطلبات الأساسية لإدارة المخاطر، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية، وتطرقت إلى المعايير الدولية التي تمت الاستعانة بها مثل (ISO/IEC 27001-27002) و (ISO 9001) و (ISO 31000) كما وتطرقت في محورها الثاني إلى الأدوار والمسؤوليات، وبينت أنّه لا بد من تحديد الأدوار الرئيسية كي تكون المؤسسة في وضع أمني فعال، وأن يكون لديها مجالات مسؤولية واضحة ومحددة، وأن تكون مفهومة، وأن تشمل منح الصلاحيات وتوضيحها للجميع في المؤسسة، وأنّها تقع على عاتق كافة الموظفين، وذكرت الوثيقة مجموعة من مسميات المسؤولين والمهام التي تقع على عاتق كلّ منهم، وثم تطرقت الوثيقة في محورها الثالث إلى تقييم المخاطر، التي تهدف لفهم كافة المخاطر الشائعة وتحديدها وتوضيحها، وهي عملية بالغة الأهمية حيث ترتكز عليها دورة صنع القرار على مستوى الإدارة، والتي تنقسم إلى قسمين: عملية تقييم المخاطر، وتتكون من أربع خطوات، تبدأ بالإعداد للتقييم ومن ثم إجراء التقييم، وبعدها اطلاع المعنيين على نتائج التقييم، ثم استمرارية التقييم، بهدف البقاء على دراية دقيقة بشأن المخاطر، وإعطاء الدرجات، من خلال استخدام معادلة المخاطر وعناصرها هي الخطر والتهديد ونقاط الضعف، واحتمال التعرض للخطر، والتأثير، ثم جاءت في المحور الرابع في ذكر بيان الرد على المخاطر، بما فيها تلك التي يمكن تقبلها في نهاية الأمر، والتي تحتاج لرد منسق ومتفق عليه، وذلك من خلال تفادي الخطر، وتقبله، وتقليل تأثيره، وتحويله، وتضمنت الوثيقة في نهايتها في المحور الخامس بيان وجوب خضوع كافة المخاطر والضوابط المطبقة للمراقبة وإعداد التقارير، فيتعين على المؤسسة أن تخضع كافة المخاطر والضوابط المطبقة لمراقبة مقررة مسبقا وتكليف الجهة المسؤولة عنها، ووضع جدول لإعداد تقارير بشأنها، ويتمّ ذلك من خلال التكليف بمتابعة الخطر، وتحديد وتيرة المراقبة، ومن ثم إعداد التقارير بشأن الخطر، ووضع نهج لمراقبة الأخطار لضمان استمرارية المراقبة.

---

[55] **المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 1 (ب) سياسة إدارة المخاطر.**

(ج): التدقيق والضمان، طرق التدقيق والحصول على الضمان (2) :[56] وتكونت هذه الوثيقة من (14) صفحة و(8) محاور تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها وثيقة ليست مستقلة دون باقي السياسات، وبيان المتطلبات الرئيسية للتدقيق والضمان، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية وتطرقت إلى المعايير الدولية التي تمت الاستعانة بها (ISO/IEC 27001-27002) و(ISO 9001)، ثم جاءت في المحور الثاني في الحديث عن بيان الدعم، والحصول على الدعم من المدراء والمعنيين الرئيسين هو في غاية الأهمية لنجاح تطبيق نظام إدارة الجودة وإجراء التدقيق، من جانب الإدارة، وذكرت الوثيقة الاعتبارات الخاصة بالمدراء، حين يلتزمون بالتدقيق والضمان، ثم تطرقت الوثيقة في محورها الثالث إلى بيان الأهداف والعمليات، فيتعين على المؤسسة أن تحدد أهداف وعمليات الجودة لكافة خدمات المؤسسة وأنشطتها، لدعم نظام إدارة الجودة في الحفاظ على مستوى مرتفع من كفاءة العمل وضمان الجودة، وتنقسم الأهداف أو الغايات إلى غايات الجودة، فهم المؤسسة والإطار الذي تعمل فيه، فهم احتياجات وتوقعات الأطراف المهتمة، وتحديد نطاق نظام إدارة الجودة، وتنقسم العمليات إلى تحسين الجودة، والتأثير على الثقافة السائدة، والتركيز على الاحتياجات التدريبية، وتطرقت في المحور الرابع إلى الحديث عن التخطيط لاستمرارية العمل، فيتعين على المؤسسة أن تضع

خططا لاستمرارية عمل أنظمتها وخدماتها في حال وقوع حادث، أو تعطل العمل، ثم جاءت في المحور الخامس في الحديث عن الضمان، بداية عن اطار الضمان، فيتعين على المؤسسة أن تضع إطارا للضمان لاستخدامه في كافة أعمال التدقيق والمراجعة والضمان لكي تتمكن من قياس عمل الأنظمة وإعطائها درجات، وليكون لديها معايير ناجحة للتحسين، مبينة لأفضل الممارسات من أجله وهي: إطار أنظمة إدارة الجودة، ونهج " التخطيط، الفعل، التحقق، اتخاذ اجراء"، ثم في نهج التدقيق والضمان، فيجب على المؤسسة نشر وإبلاغ كافة الأطراف المعنية بشأن الطريقة التي تخطط بها للتدقيق والضمان، وبالطرق التي تتبعها لقياس الضوابط ومراجعتها، أي بقياس الضمان، ومراجعة الضوابط، كما تطرقت الوثيقة في المحور السادس إلى جداول التدقيق وأنماطها، فيجب أن يكون هناك جدول للتدقيق محدد سلفا، يتضمن كافة أنماط التدقيق التي تجرى، وكافة أعمال التدقيق والفرق التي تنفذها، وطريقة إعداد تقارير بالنتائج، وكيفية استيفاء المتطلبات الالزامية، وتنقسم إلى: وضع الجداول، وأنماط التدقيق، وإعداد تقرير بالنتائج، ووضع واجبات قانونية لعمليات

[56] المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 1 (ج) سياسة التدقيق والضمان.

التدقيق، وبينت الوثيقة في المحور السابع، سجلات التدقيق، فيتعين على المؤسسة أن تنشئ سجلات تدون فيها كافة نتائج التدقيق، وادارتها وحفظها بشكل آمن بما يتناسب مع حساسية تلك النتائج ونقاط الضعف التي تكشف عنها، وباعتبارات أخرى على عملية التدقيق، مثل المساءلة والاستقلالية، والمسؤوليات، والصلاحيات، ومقاييس ممارسات التدقيق، وفي النهاية تضمنت الوثيقة في المحور الثامن والأخير التخطيط للمراجعات الأمنية والتحسين المستمر، حيث يتعين على المؤسسة أن تضع الخطط لإجراء مراجعات أمنية منظمة وأعمال تحسين مستمر، لكي تكسب النضج وتتطور بما ينسجم مع غايات التحسين.

(د): الامتثال الدولي، المعايير اللازمة للتعاون الدولي (1)[57]: وتكونت هذه الوثيقة من (15) صفحة و (4) محاور تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها وثيقة ليست مستقلة دون باقي السياسات، وبيان المتطلبات اللازمة لأجل الامتثال الدولي، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية، وأن هذه السياسية صيغت بشكل مختلف لتوفر مصدرا واحدا للمعايير الدولية، وبيان الإيجابيات والسلبيات عند اتباع المعيار الدولي، وتطرقت في المحور الثاني إلى المعايير الدولية التي تمت الاستعانة بها وهي معايير ISO/IEC وتضمنت كلّ من:(ISO/IEC 9001)، (ISO 10007:2017)، (ISO/IEC 19770-1:2017)، (ISO/IEC 20000)،(ISO 22301)،(ISO/IEC 27001-27002) (ISO/IEC 27031)، (ISO/IEC 28000)، (ISO 55000)، والمعايير البريطانية/الأوربية، وتضمنت كلّ من: (BS EN 1143)، (BS EN 1300)، (BS EN 1627)، (PAS 24)، وتحدثت عن اعتماد الأفراد، ومن الأمثلة على السبل المحددة التي يمكن للأفراد اتباعها للحصول على اعتماد بمجال ممارسة الأمن، (IISP)، (SANS)، كما تحدثت الوثيقة في محورها الثالث عن التوجيهات والإرشادات، فيتعين على المؤسسة أن تكون منفتحة على تطبيق التوجيهات وعازمة على استيفاء المعايير ومستويات الاعتماد، فتنشر كافة الأهداف وتدخلها في سجلاتها حتى يتمكن كافة العاملين من تحقيق تلك الأهداف من خلال درايتهم بها، والمعايير مثل معايير ومطبوعات المعهد الوطني للمعايير والتكنولوجيا، وهي: (NIST SP 800-30) (المراجعة 1)، (NIST SP 800-53A -تقييم الضوابط الأمنية) (المراجعة 2)، NIST SP 800- (60)، (NIST SP 800-175A and 800-175B)،(NIST AES)، (NIST SP 800-115- الاختبار والتقييم)، NIST SP 800-161- سلسلة الموردين)، ومجموعة ضوابط أمن العاملين، وفيها، تدابير أمن العاملين،

[57] المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 1 (د) سياسة الامتثال الدولي.

وتصنيف شاغلي المناصب، والتدقيق الأمني في العاملين، وإنهاء خدمات العاملين، واحتوى المحور الرابع على تطبيق أطر العمل، لوضع تصور لكيفية دعم هذه السياسات لبعضها البعض، وعرض لأطر عمل أفضل الممارسات المعترف بها دوليا، وهي: إطار عمل المعهد الوطني للمعايير والتكنولوجيا(NIST) بشأن إدارة المخاطر، مكتبة البنية التحتية لتكنولوجيا المعلومات، إطار مخاطر تكنولوجيا المعلومات-جمعية تدقيق أنظمة المعلومات وضبطها، (ISACA)، غايات ضوابط المعلومات والتكنولوجيا المصاحبة لها (COBIT)، وتشمل إطار العمل، وتوصيف العمليات، وغايات الضوابط، والتوجيهات الإرشادية للإدارة، ونماذج النضوج. ثم الاعتبارات الأساسية.

المجال الأساسي 2: العلامات الوقائية، وتوفير الموارد، وضبط الأصول، والتي تكون من أربع وثائق وهي:

(أ): نظام العلامات الوقائية، نظام التصنيف المتبع، بما في ذلك التعامل مع المعلومات بطريقة خاصة ومعايير التطبيق(1)[58]: وتكونت هذه الوثيقة من (8) صفحات ومحورين تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها وثيقة ليست مستقلة دون باقي السياسات، وبيان المتطلبات الأساسية لنظام العلامات الوقائية، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية، وتطرقت إلى المعايير الدولية التي تمت الاستعانة بها مثل (ISO/IEC 27001-27002) و (NIDT SP 800-60)، كما وتطرقت في محورها الثاني إلى بيان تنفيذ نظام العلامات الوقائية، والذي ينقسم إلى كلّ من: الاستخدام الصحيح للتصنيف، فيتعين على المؤسسة أن تحدد علامات التنصيف الصحيحة، والأكثر ملائمة لكافة أصولها ومعلوماتها وبياناتها حسب حساسيتها وأهميتها للمؤسسة، وحسب برنامج تصميم محدد مسبقا، لضمان توفير الحماية الدائمة والمتناسبة مع أهمية تلك الأصول، وبإدارة المخاطر، وذكرت الوثيقة مستويات التصنيف المستخدمة في الأردن، مع شروحات عن شدة التأثيرات المصاحبة للأخطار، ثمّ الضوابط الأمنية، كوضع قواعد للدخول إلى الأصول، وحماية أمنية الزامية كالتشفير، ثمّ الحماية الإضافية، وتطبيق تصنيفات العلامات الوقائية ، فيجب أن تحمل كافة الأصول التي تعتمد عليها المؤسسة في أداء عملها اليومي وتيسير مصالحها علامات وقائية ملائمة تحدد

---

[58] **المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 2 (أ) سياسة نظام العلامات الوقائية.**

تصنيفها وفق ما حدده الشخص المسؤول عن الأصول، ثمّ إزالة التصنيف، وفي نهاية الوثيقة الاعتبارات الرئيسية.

(ب): الحماية والإفصاح، الضوابط المتعلقة بالأصول والمعلومات وتصنيفها، والإفصاح عنها(2)[59]:

وتكونت هذه الوثيقة من (10) صفحات ومحورين تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها وثيقة ليست مستقلة دون باقي السياسات، وبيان المتطلبات اللازمة للحماية والإفصاح، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية، وتطرقت إلى المعايير الدولية التي تمت الاستعانة بها مثل (ISO/IEC 27001-27002) و (NIDT SP 800-60)، كما وتطرقت في محورها الثاني إلى بيان تطبيق الحماية والإفصاح، فيتعين على المؤسسة أن تحدد النهج الذي ستتبعه وطريقة تطبيق الحماية والإفصاح، والذي يمكن تحقيقه عن طريق استخدام كلّ من: سجلات الأصول، ثمّ من خلال تطبيق التصنيفات، فيتعين على المؤسسة أن تحدد بشكل واضح الطرق والإرشادات التي تتبعها لوضع معايير تطبيق تصنيف الأصول، ثمّ تقييم الأثر على كافة الأصول، ثمّ إعطاء علامات وقائية لكافة الأصول التي تخضع للتصنيف حسب

مستوى تصنيفها وإلى جانب متطلبات التعامل معها بطريقة خاصة، ثمّ توعية الموظفين، فيتعين على المؤسسة أن تطلع كافة الموظفين المعنيين بالتعامل مع الأصول ونقلها وتخزينها ، ثمّ المراجعات الدورية على كميات الأصول التي لدى المؤسسة والضوابط التي تم تأسيسها وتحتاج لمراجعات دورية للتأكد من صلاحيتها وفاعليتها، ثمّ الإفصاح، بوضع قواعد وإرشادات لتسهيل الإفصاح الآمن والمصرّح به بالشكل الملائم، وفيها يجب وضع تدابير تأديبية ملائمة وهي: اتفاقيات عدم الإفصاح، ومدد الإفصاح، واعتبارات رئيسية، وفي نهاية الوثيقة تم إلحاق نموذج لسجل الأصول.

(ج): إدارة الموارد، ضمانات الموردين والعلاقات معهم(1)[60]: وتكونت هذه الوثيقة من (11) صفحة وانقسمت إلى ثلاث محاور تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها وثيقة ليست مستقلة دون باقي السياسات، وبيان المتطلبات الرئيسية لإدارة الموارد، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية، وتطرقت إلى المعايير الدولية التي تمت الاستعانة بها مثل (ISO/IEC 27001 and 27002) و

---

[59] المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 2 (ب) سياسة الحماية والإفصاح.

[60] المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 2 (ج) إدارة الموارد.

(NIDT SP 800-53)، (ISO/IEC 28000)، (ISO/IEC 9001)، كما تطرقت في محورها الثاني إلى بيان إدارة الموارد، والذي ينقسم إلى: تطبيق إدارة الموارد، وعملية شراء آمنة، فيتعين على المؤسسة أن تحدد عملية للشراء لضمان شراء السلع والخدمات بشكل آمن من المزودين، ويجب أن تشمل العملية إجراءات كفيلة بالحد من المخاطر المحيطة بعملية الشراء؛ ثم إدارة دورة حياة الموارد، بتعيين تطبيق إجراءات رسمية لتوحيد معايير إدارة دورة حياة العلاقة مع المزودين في كافة قطاعات المؤسسة، ووضع شرح مفصل عن الأنشطة المحددة والمسؤوليات المتعلقة بها، ثمّ ضمان سلسلة التوريد، بتحديد مجموعة من المعايير الأمنية للمزودين من أجل تقييم ملاءمتهم، وهذا يوفر ضماناً أمنيًّا على كافة مستويات سلسلة التوريد، كما جاءت الوثيقة في محورها الثالث في بيان العلاقات مع المزودين، من خلال: المراجعة بشأن المزودين قبل الطلب، أي تجري مراجعة بشأن أوضاع المزود قبل الدخول في اتفاق تعاقدي معه، بما في ذلك تصميم السلع واختبارها وتسليمها، وتقييم تدرب وخبرات موظفي المزودين، وإجراء مراجعات فنية للسلع، على سبيل المثال، وضمان أمن المزودين، بتسجيل وحفظ كافة المعلومات والمتطلبات الأمنية المتعلقة بما تم الاتفاق عليه، وتغييرات المزودين، فيتعين على المؤسسة الاتفاق على أية تغييرات لأحكام توفير الخدمات من جانب المزودين، وأن يتم تدوينها وادارتها، مع مراعاة حساسية المعلومات التي تخص عمل المؤسسة، وإعادة تقييم كافة المخاطر، ثمّ الامتثال والمراجعات بشأن المزودين، أي بمراجعة دورية وعمليات تدقيق لأسلوب المزود في تقديم الخدمات لضمان أن السلع والخدمات والعقود كافية تفي بالغرض، ثمّ تحديد أحكام إنهاء العقد، بوضع عملية واضحة لإنهاء العقود، وتطبيقها بشكل ثابت على كافة العقود مع المزودين، ثمّ الاعتبارات الرئيسية.

المجال الأساسي 3: أمن الأفراد، والذي تكون من وثيقتين وهما:

(أ): معايير أمن الأفراد، طرق التقديم على تصريح أمني، والتدقيق به، وتجديده، ومراجعته، وسحبه[(2)]:[61] وتكونت هذه الوثيقة من (9) صفحات و (4) محاور تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها وثيقة ليست مستقلة دون باقي السياسات، وبيان المتطلبات الأساسية لمعايير أمن الأفراد، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية، وتطرقت إلى المعايير الدولية التي تمت الاستعانة بها مثل: (NIST SP 800-53 أمن الأفراد)،

[61] المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 3 (أ) سياسة معايير أمن الأفراد.

وتطرقت الوثيقة في محورها الثاني إلى التعريف المسبق لأمن الأفراد، بتحديد وتأسيس نهج مدروس لأمن الأفراد، لضمان أمنهم، ثم تطرّقت الوثيقة في محورها الثالث إلى بيان دورة التوظيف، مقسّمة إلى قسمين: قبل التوظيف، أي بإجراء تحقيق وتدقيق أمني في خلفية أي موظف قبل توظيفه، وعمليات التدقيق تصنف إلى: التدقيق الأمني في خلفيات الأفراد، التدقيق الأمني الأساسي في خلفيات الموظفين، التدقيق الأمني المتقدم في خلفيات الموظفين، ثمّ يأتي القسم الثاني وهو مراحل التوظيف، وفيه، توفير التدريب الأولى للتوعية الأمنية، فيتعين على المؤسسة توفير تدريب مناسب لضمان توعية الموظفين الجدد والعاملين أصلا فيها بشأن التدابير الأمنية ومسؤولياتها حيالهم، والمراجعات الدورية للتدقيق الأمني، فينبغي أن تجرى مراجعات في خلفيات الموظفين الحاليين في المؤسسة، بموجب جداول زمنية محددة، وتتناسب مع مستوى التصريح الأمني للموظف، والتدريب والتواصل والمراقبة وإعداد التقارير باستمرار بشأن التوعية الأمنية، ثمّ الإحاطة المتعلّقة بانتهاء الخدمة أي العمل لدى المؤسسة، بعمل بلورة يمكن من خلالها إحاطة الموظف لدى انتهاء خدمته بها، وتوعيته بمسؤولياته، أو التزاماته بعد خروجه منها، وجاءت في محورها الرابع تتحدث عن الاعتبارات الأساسية.

(ب): التصريح الأمني، مستويات التصريح الأمني ومدته [(1)] :[62] وتكونت هذه الوثيقة من (8) صفحات و(3) محاور و تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها وثيقة ليست مستقلة دون باقي السياسات، وبيان المتطلبات اللازمة للحصول على تصريح أمني، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية، وتطرقت إلى المعايير الدولية التي تمت الاستعانة بها وهي (NIST SP 800-53 – أمن الأفراد)، وتطرقت الوثيقة في محورها الثاني إلى بيان إصدار التصاريح الأمنية، من خلال تحديد مستويات التصريح الأمني، فيتعين على المؤسسة أن تحدد بوضوح التسلسل الهرمي لمستويات التصريح، واعتماد عمليات التدقيق الأمني في خلفيات الأفراد الواجب قيامهم بها، وينقسم إلى قسمين: التصريح الأمني، بوجوب إصدار تصريح أمني مناسب للأفراد يتناسب مع أعلى مستوى من التصنيف الأمني للمعلومات، أو الأصول الأمنية التي يمكنهم الاطلاع عليها بلا ضوابط، والأطراف الثالثة، بإجراء تدقيق أمني في خلفيات أطراف ثالثة، سواء من المزودين أو الزائرين، الذي يمكنهم الاطلاع على بيانات حساسة أو تملكها المؤسسة، ثمّ المراجعات الدورية للتصاريح الأمنية، أي للأفراد الذين صدرت لهم تصاريح أمنية، وذلك لضمان أن يكون مستوى التصريح الأمني الصادر لهم ما زال لازما وملائما، ثمّ في النهاية تحديد مدة صلاحية التصريح الأمني

---

[62] **المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 6 (ب) سياسة التصريح الأمني.**

وتجديده، فيتعين على المؤسسة تحديد مدة صلاحية للتصريح مناسبة لكل مستوى، ويلزم على الأفراد تقديم طلبات لتجديد تصاريحهم الأمنية لدى انتهاء صلاحيتها، وانتهت الوثيقة في محورها الثالث للحديث عن الاعتبارات الرئيسية.

المجال الأساسي 4: أمن الأفراد، والتي تكون من خمس وثائق وهي:

(أ): أمن المعلومات، حماية المعلومات المتداولة والمنقولة والبيانات المحفوظة، بما في ذلك التخزين بمنصات عبر الانترنت وعلى الأجهزة، والاستخدام المقبول [2]:[63] وتكونت هذه الوثيقة من (15) صفحة و (4) محاور تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها وثيقة ليست مستقلة دون باقي السياسات، وبيان المتطلبات الأساسية لأمن المعلومات، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية، وتطرقت إلى المعايير الدولية التي تمت الاستعانة بها

مثل: (ISO/IEC 27001-27002)، (NIST SP 800-175A – 800-175B)، وتطرقت الوثيقة في محورها الثاني إلى نظام إدارة أمن المعلومات (ISMS)، من خلال وضع نظام لإدارة أمن المعلومات، بوضع نظام خاص يحدد الضوابط الفنية وغير الفنية التي تعتزم تطبيقها لمعالجة المخاطر ولضمان استمرارية عملها وأمن معلوماتها، ومن خلال نطاق حدود ونظام إدارة أمن المعلومات، الذي يجب أن يغطي الجوانب التالية: كافة أصول المعلومات المخزنة أو المعالجة على منصات المعلومات أو تكنولوجيا المعلومات، وكافة أصول المعلومات التي يعالجها ويخزنها الموظفون لصالح المؤسسة، وأصول المعلومات الموكل بها للموظفين من قبل الشركاء، والأطراف الثالثة، كما جاءت في محورها الثالث للحديث عن تطبيق نظام لإدارة المعلومات ولتحقيقه، لا بدّ من تحقيق حماية البيانات الحية والمنقولة، فيتعين على المؤسسة وضع سياسات وإجراءات رسمية لنقل البيانات، وإرساء ضوابط لحماية نقل المعلومات من خلال استخدام كافة أصناف ووسائل نقلها، ثمّ الاستخدام الآمن للبريد الالكتروني والاتصالات، ثمّ انشاء أنظمة لتخزين البيانات، بتخزينها على الانترنت والأقراص الصلبة، لحماية البيانات غير المتداولة، واسترجاعها بطريقة واطار زمني مقبول، كالتخزين على منصة Cloud وعلى الإنترنت، والتخزين محليًّا، والتخزين خارج نطاق الانترنت وأجهزة التخزين المحمولة، ثمّ تحديد استخدام ضوابط التشفير لحماية المعلومات وتطويرها وتطبيقها وينقسم إلى: تشفير البيانات، وإدارة المفاتيح، وأساليب أخرى، مثل خوارزمية دالة

---

[63] **المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 4 (أ) سياسة أمن المعلومات.**

هاش (Hashing)، ثمّ التحكم بالدخول إلى البيانات، من خلال حقوق ضوابط الدخول إلى البيانات، بوضع قواعد فيما يخص انشاء سجل رسمي بالأشخاص الذين يدخلون إلى البيانات، وشطب أسماء من لم يعد لهم حق بذلك، ومن خلال تحديد قواعد كلمة السر، بوضع ضوابط صارمة بشأن إنشاء واستخدام وتخزين كلمات السر للموظفين، ثمّ الاستعمال المقبول للبيانات والأصول، بوجوب إرساء قواعد محددة للاستخدام المقبول للمعلومات، والأصول المتعلقة بالمعلومات، ومرافق معالجة المعلومات، ثمّ اتفاقيات الحفاظ على السرية وعدم الإفشاء، التي تعكس احتياجات المؤسسة لحماية المعلومات، وتوثيق تلك المتطلبات ومراجعتها دوريا، ثمّ تطرقت الوثيقة في محورها الرابع إلى الاعتبارات الرئيسية، وتمّ إلحاق دليل معيار (ISO27001) لأفضل الممارسات لنظام إدارة أمن المعلومات.

(ب): ضمان المعلومات، الحصول على اعتماد رسمي واستيفاء متطلبات التدقيق (1) :[64] وتكونت هذه الوثيقة من (10) صفحات و (4) محاور تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها وثيقة ليست مستقلة دون باقي السياسات، وبيان المتطلبات الأساسية لضبط المعلومات، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية، وتطرقت إلى المعايير الدولية التي تمت الاستعانة بها مثل: (ISO/IEC 27001-27002)، (ISO/IEC 9001)، وتطرقت الوثيقة في محورها الثاني إلى الحديث عن تطبيق ضمان المعلومات، من خلال التقييم والتطوير والتنفيذ والضبط، وينقسم إلى: مبادئ ضمان المعلومات، فينبغي على المؤسسة أن تضع خطة للتعامل مع أمن وضمان المعلومات، على أن يشمل ذلك كافة الضوابط المطلوبة لتحقيق الالتزام والكفاءة، ثمّ ضبط دورة حياة البيانات، بتطوير عمليات وإجراءات لحماية وضمان البيانات بالشكل الملائم في كافة مراحل دورة حياة البيانات منذ انشائها وحتى إتلافها، ثمّ اختيار خط الأساس فعلى المؤسسة أن تختار خط أساس للجوانب الأمنية ونظام اعتماد مناسب، لكي تتمكن من قياس ما تحققه من تقدم وتحسن، ثمّ القيم الأساسية لضمان المعلومات، سريتها، توافرها، سلامتها، التحقق منها، وعدم الانكار، ثم تطرقت الوثيقة في محورها الثالث للحديث عن توثيق المعلومات، فينبغي على المؤسسة أن تتأكد من وجود ضوابط لضمان أن تكون

كافة الاتصالات قد جرى توثيقها، ويشمل ذلك نقل الوثائق والتغييرات في وسائط نقلها، وتوليف أنظمة المعلومات، كما جاءت في محورها الرابع للحديث عن عدم القدرة على الإنكار، فلا يمكن لأي فرد أن ينفي

[64] **المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 4 (ب) سياسة ضمان المعلومات.**

وقوع عمل ما، من خلال إنشاء جداول للتدقيق الداخلي والخارجي، تستند إليها آلية الضمان وعدم القدرة على إنكار التغيير، ثمّ النسخ الاحتياطي عن البيانات، فيتعين على المؤسسة وضع جداول زمنية منتظمة لحفظ نسخ احتياطية عن كلّ من الوثائق والبيانات، وتوليف البرامج والشبكة، ولا بدّ من الالتزام بتلك الجداول، ثمّ الاعتبارات الرئيسية.

(ج): إدارة توليف الشبكات، توليف الشبكات والدخول فيها(1):[65] وتكونت هذه الوثيقة من (13) صفحة وانقسمت إلى خمسة محاور تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها وثيقة ليست مستقلة دون باقي السياسات، وبيان المتطلبات الأساسية لإدارة توليف الشبكات، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية، وتطرقت إلى المعايير والأطر الدولية التي تمت الاستعانة بها مثل: (ISO 10007:2017)، (ISO/IEC 19770-1:2017) (ISO/IEC 20000)،(ISO/IEC 27001/2)، مكتبة البنية التحية لتكنولوجيا المعلومات(ITIL)، وتطرقت إلى الأصول الحساسة للشبكة وإدارة توليف الشبكات، ثم جاءت الوثيقة في محورها الثاني للحديث عن تنفيذ إدارة توليف الشبكات، وذلك من خلال تحديد نطاق إدارة توليف الشبكات، فعلى المؤسسة أن تحدد نطاق مصادر المعلومات المتعلقة بتوليف الشبكة ليتم تسجيلها، والحفاظ عليها حسب نمط كل أصل، وحساسيته لعمليات المؤسسة واستمراريتها، ومن خلال الربط بين الشبكة والأصول الذي ينقسم إلى كلّ من: الأصول الحساسة في الشبكة، بتحديد أصول الشبكة والعمل على إعداد وحفظ قائمة بها، وتحديد حساسية تلك الأصول وقسم ترابط الشبكة، بعمل رسوم توضح بدقة ترابط الشبكة، وتحديد الأشخاص المسؤولين عنها، كما جاءت الوثيقة في المحور الثالث تتحدث عن الحوكمة وإعداد التقارير، فيتعين على المؤسسة وضع هياكل واضحة للحوكمة وإعداد التقارير، ووجوب إطلاع كافة الأفراد المعنيين عليها، بمن فيهم المسؤولين مع تحديد المسؤوليات عن كافة الأصول، بتنفيذ الهياكل وتحديد مسؤوليات المستخدمين، والحرص على شراء المنتجات والخدمات من قنوات مناسبة، وفي المحور الرابع جاءت للحديث عن ضبط توليف الشبكات بتسجيل عمليات تغيير توليف أجهزة الشبكة أو أية أصول أخرى، مع شمول حيثيات التغير وأسبابه، ثمّ حفظ السجلات وتدقيقها باستمرار، إمّا يدويا أو باستخدام أنظمة إدارة توليف الشبكات(CMS)، ويتعين مراجعتها بانتظام ومقارنتها مع التوليفات والنسخ الحالية لضمان أنّ هناك تسلسل واضح لأعمال التدقيق على التغييرات المصرح بها التي تم اجراؤها، وفي نهاية الوثيقة في آخر محور لها المحور الخامس، بينت وجوب إدارة

---

[65] **المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 4 (ج) إدارة توليف الشبكة.**

نقاط الضعف، فيتعين على المؤسسة جمع المعلومات عن نقاط الضعف التقنية والابلاغ عنها بالتوقيت المناسب، وتقييم انكشاف المؤسسة على نقاط الضعف المعروفة، واتخاذ الإجراءات للتصدي للمخاطر التي تنشأ عنها، ويتم ذلك من خلال تقييم نقاط الضعف ثمّ اعداد التقارير والمعلومات، والاستجابة لنقاط الضعف، ثمّ تطوير عملية تصحيح البرامج، بوضع جدولا زمنيا لتنزيل التصحيحات بما في ذلك عملية تقييم المخاطر، بتنزيل تصحيح جديد على نظام ما، واتخاذ القرار بشأن ما إذا كان من المناسب تنزيله، وفي نهايتها الاعتبارات الرئيسية.

(د): الأجهزة المحمولة، استخدام أجهزة تخزين المعلومات ونقلها وتدوينها[1]:[66] وتكونت هذه الوثيقة من (9) صفحات وانقسمت إلى محورين تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها وثيقة ليست مستقلة دون باقي السياسات، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية، وتطرقت إلى المعايير والأطر الدولية التي تمت الاستعانة بها مثل: (ISO/IEC 27001 and 27002)، وبينت في محورها الثاني استراتيجية الأجهزة المحمولة وذكرت أنه يجب على كل مؤسسة وضع سياسة وإجراءات أمنية من أجل إدارة المخاطر التي تنشأ عن الأجهزة المحمولة وتبين الحالات التي يمكن أو التي لا يمكن من خلالها استخدام الأجهزة المحمولة وبينت أمثلة من أنواع الأجهزة المحمولة، وبينت سياسة الاستخدام المقبول والمناطق الأمنة والضوابط التقنية والمادية في الأجهزة المحمولة والإدارة التقنية لتلك الأجهزة ووضحت الآليات المتبعة في استخدام الأجهزة المحمولة المملوكة للمؤسسة والأجهزة الخاصة التي يستخدمها الموظفون، وتحدثت عن أدوات الاحتواء ودورة حياة الأجهزة المحمولة، ومن ثم ذكرت أهم الاعتبارات الأساسية في هذا الموضوع.

(ه): المراقبة الوقائية، فرض تنفيذ السياسيات، كشف حالات الاختراق[2]:[67] وتكونت هذه الوثيقة من (13) صفحه وانقسمت إلى محورين تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وتحديد أهم المتطلبات من أجل تطبيقها وبيان انها وثيقة ليست مستقلة دون باقي السياسات، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية، وتطرقت إلى المعايير والأطر الدولية التي تمت الاستعانة بها مثل: (ISO/IEC 27001 and 27002) و (ISO/IEC 27031) ، وبينت في محورها الثاني ألية تنفيذ المراقبة الوقائية وبيان الضوابط

[66] **المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 4 (د) سياسة الأجهزة المحمولة.**

[67] **المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 4 (هـ) سياسة المراقبة الوقائية.**

الأساسية لتنفيذ المراقبة الوقائية مثل مراقبة النظام و مراقبة حركة الشبكة ومراقبة الفعاليات التي يقوم بها المستخدم وأشارت إلى أنه لابد من الرجوع إلى وثائق أخرى قديمة لكنها لاتزال معتمدة وبينت مجموعة من الضوابط التي لابد من التأكد منها كونها تعتبر مفيدة للمؤسسات من أجل استخدام البنى التحتية بالشكل الأمثل. ثم انتقلت للتحدث عن إدارة السجلات وبينت فيها أنه لابد من اختيار وتدوين سجلات نشاط الشبكة وأن هذه السجلات يتم تجميعها من خلال خدمات الشبكات والبنى التحتية للشبكات والبنى التحتية لأنظمة التشغيل والتطبيقات ومن عمليات الاتصال بالشبكة عن بعد، ثم تحدثت عن محتويات سجل نشاط الشبكة وأهم التفاصيل الضرورية الممكن وضعها داخلها ومن ثم تحدثت عن تخزين وحماية السجلات، وتطرقت السياسة إلى عملية تحليل السجلات وحالات الاستخدام وكيفية الاستفادة منها في التعرف على حالات الاستخدام والاستعانة بالمعلومات بشأن التهديد وكذلك تحدثت عن عملية تحليل السجلات وأهم الفوائد التي يتم تحقيقها من خلال تحليل السجلات، وبينت السياسة بعد ذلك ألية مراقبة العمليات من خلال مراقبة الموظفين اثناء استخدامهم لأنظمة المعلومات وهل تتم ضمن المعايير والضوابط المعتمدة وتوعية الموظفين حول الأخطار المتوقعة ومن ثم تحدثت عن مراقبة الأصول و مراقبة الأجهزة المتلقية للبيانات وأهم الوسائل المتبعة لذلك وفي الختام تحدثت عن أهم الاعتبارات الأساسية لتطبيق هذه السياسة.

المجال الأساسي 5: الأمن المادي، والذي تكون من ثلاث وثائق وهي:

(أ): الوسائل الدفاعية المتعمقة، تأمين محيط الموقع، وتطبيق مستويات من الأمن(1):[68] وتكونت هذه الوثيقة من (16) صفحه و (6) محاور أساسية تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها وثيقة ليست مستقلة دون باقي السياسات، وبيان المتطلبات الأساسية لتطبيقها، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية، وتطرقت إلى المعايير والأطر الدولية التي تمت الاستعانة بها مثل: (ISO/IEC 27001و27002)، و (ISO 22301) وفي محورها الثاني تحدثت عن تطبيق الوسائل الدفاعية المتعمقة وأنه لابد لكل مؤسسة من تطوير نهج للوسائل الدفاعية ضد الهجمات السيبرانية خصوصا محاولات اختراق سرية وحساسية الأصول المعلوماتية ويتم ذلك من خلال فهم مستويات الحماية مثل مستوى حماية الإجراءات ومستوى الحماية المادية ومستوى الحماية التقنية ومن خلال تقسيم الحماية إلى مستويات سيتذكر في وثائق أخرى وكذلك لابد من وضع الاستعدادات الأمنية مثل المراقبة والتدريب والتوعية والتحليل وغيرها، وبينت في

---

[68] **المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 5 (أ) سياسة الوسائل الدفاعية المتعمقة.**

محورها الثالث كيفية تقسيم الحماية الإجرائية إلى مستويات مثل الامتثال للسياسة المتبعة وتأهيل الكفاءات والتدريب، وفي محورها الرابع تحدثت عن تقسيم الحماية المادية إلى مستويات مثل محيط الموقع وكيفية حمايته ومن ثم المداخل وكيفية حمايتها ومن ثم تشكيل فرق الاستجابة للحوادث والتي تم تقسيمها إلى أكثر من فريق مثل فريق الاستجابة للحوادث السيبرانية و الفرق الأمنية، وفي محورها الخامس تحدثت عن تقسيم الدفاعات التقنية إلى مستويات ومن أجل ذلك لابد من فهم الشبكة والأصول المعلوماتية ومن ثم تحديد المحيط الفعلي للشبكة وتحديد حركة البيانات وتحديد التهديدات وانتقاء المنتجات والخدمات وبيان طريقة اعداد التقارير وطريقة الاستجابة للحوادث وعملية المراقة والرد، وبعد تحديد وفهم الشبكات والأصول يتم العمل على مستويات متعددة لحماية الشبكة مثل أمن المحيط و أمن الشبكة وأمن نقطة الاستقبال وأمن التطبيقات وأمن البيانات، وفي المحور السادس تحدثت الوثيقة عن الاعتبارات الأساسية لتطبيقها وتم الحاق نموذج لدورة الهجوم السيبراني .

(ب): الحاويات والتخزين، متطلبات أمن الأثاث والحجرات والتخزين[2]:[69] وتكونت هذه الوثيقة من (8) صفحات و (3) محاور أساسية تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها وثيقة ليست مستقلة دون باقي السياسات، وبيان المتطلبات الأساسية لإدارة التغيير، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية، وتطرقت إلى المعايير والأطر الدولية التي تمت الاستعانة بها مثل: (ISO/IEC 27001و27002)، و (B EN 1143) و (BS EN 1627وPAS 24) وفي محورها الثاني ضبط الحاويات والتخزين والتي تضمنت التوجيهات والإرشادات من أجل الحاويات والتخزين مثل الموقع الأمن والتي تحدثت عن الأمن المادي للموقع وتحدثت عن إجراء دراسات من أجل تشييد المباني والغرف والالتزام بالمعايير الخاصة بذلك والتأكد من استخدام الأثاث الأمن ومواصفات الأثاث مثل الخزائن و والتمديدات الكهربائية وحوافظها وغيره وتطرقت في المحور الثالث إلى أهم الاعتبارات الرئيسية من أجل هذه السياسة.

(ج): الدخول إلى الموقع، ضبط الدخول إلى الموقع، وضبط الزائرين[1]:[70] وتكونت هذه الوثيقة من (10) صفحات و (3) محاور أساسية تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها

---

[69] المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 5 (ب) سياسة الحاويات والتخزين.

[70] المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 5 (ج) سياسة الدخول إلى الموقع.

وثيقة ليست مستقلة دون باقي السياسات، وبيان المتطلبات الأساسية لإدارة التغيير، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية، وتطرقت إلى المعايير والأطر الدولية التي تمت الاستعانة بها مثل: (ISO/IEC 27001و27002)، وفي محورها الثاني تحدثت عن تطوير مستويات الدخول المادي بما فيها من ضوابط تقييد الدخول و تحديد الحدود الأمنة للموقع والمستويات الأمنة للدخول وكيفية ضمان تطبيق الإجراءات المتعلقة بذلك وتحديد الضوابط الداخلية ومسؤوليات الموظفين وسياسات إخلاء سطح المكتب وتغطية لوحات الأرقام السرية ومن ثم ألية تنظيم دخول الزائرين وحفظ سجلات الدخول وعملية مراقبة الزائرين وكيفية التعامل معهم وكذلك تحدثت عن ألية تنظيم المزودين وعمليات استلام السلع وعماية استلام الشحنات ووضع وإدارة المتطلبات الأمنية من اجل اتفاقيات التوريد والصيانة، وفي محورها الثالث تحدثت عن أهم الاعتبارات الأساسية لتطبيق هذه السياسة.

المجال الأساسي 6: استمرارية العمل، والذي تكون من ثلاث وثائق وهي:

(أ): إدارة التغيير: التخطيط للتغيير، والإعلانات بشأنه، وإحداثه، وتعميمه(2):[71] وتكونت هذه الوثيقة من (13) صفحة و (7) محاور أساسية تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها وثيقة ليست مستقلة دون باقي السياسات، وبيان المتطلبات الأساسية لإدارة التغيير، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية، وتطرقت إلى المعايير والأطر الدولية التي تمت الاستعانة بها مثل: (ISO 9001)، و (ITIL) مكتبة البنية التحتية لتكنولوجيا المعلومات و (NIST SP 115-800) الاختبار والتقييم وفي محورها الثاني تحدثت عن تطبيق إدارة التغيير خصوصا مع ارتفاع حالات اكتشاف نقاط الضعف في البرمجيات فعليه لابد من إدارة التغيير بفعالية من أجل الحفاظ على سلامة المعلومات وسريتها وأنه لابد من تشكيل لجان استشارية للتغيير في كافة المؤسسات وبينت الهيكل التنظيمي لهذه اللجان ووتيرة عقدها للاجتماعات وأدوار أعضائها وتحدثت في محورها الثالث عن نطاق التغيير وأنه لابد لكل مؤسسة من بيان النقاط التي ضمن أو خارج نطاق التغيير وبيان ماهي هذه النقاط وفي محورها الرابع تحدثت عن طلب التغيير وأنه لابد للمؤسسات من استخدام استمارات من اجل طلب التغيير تبين كافة المعلومات المطلوبة وعلية ستتم دراسة الطلبات وإعطاء موافقة مبدئية ثم تتم عملية تقييم أثر التغيير وتحديد أولوية طلب التغيير وفي محورها الخامس تحدثت عن التخطيط للتغيير وتنفيذه وبينت أنه توجد خطط للتراجع عن التغيير وإعادة النظام إلى وضعه السابق وتحدثت

---

[71] **المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 6 (أ) إدارة التغيير.**

عن عملية اختبار التغيير والإشعار بالتغيير، ومن ثم تحدثت عن التنفيذ وفي محورها السادس تحدثت عن مراجعة مدى القبول بالتغيير وفي محورها الأخير تحدثت عن اهم الاعتبارات الأساسية في هذه العملية.

(ب): الاستجابة لدى وقوع حادث: تحليل الحوادث، وتصعيدها للمستوى المطلوب، والاستجابة بعد وقوعها[(1)]:[72] وتكونت هذه الوثيقة من (17) صفحة و (6) محاور أساسية تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها وثيقة ليست مستقلة دون باقي السياسات، وبيان المتطلبات الأساسية ، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية، وتطرقت إلى المعايير والأطر الدولية التي تمت الاستعانة بها مثل: (ISO 22301)، و (ISO/IEC 27001و27002) و (ISO/IEC 9001) ، وتحدثت في محورها الثاني عن التخطيط للاستجابة لوقوع الحوادث السيبرانية وتنفيذها وبيان الأخطار التي لابد من وضع الخطط لها مثل الإضرار بالعمل أو العرقلة المستمرة أو عدم الامتثال للمتطلبات القانونية والتنظيمية بشأن الإبلاغ، وتحدثت في محورها الثالث عن المسؤوليات والقدرات وأنه لابد لكل مؤسسة أن توجد إمكانات للاستجابة لمثل هذه الحوادث سوآءا كانت داخلية أو خارجية وبيان الأدوار والمسؤوليات للمعنيين بالاستجابة و تدريب فريق الاستجابة للحوادث والتوعية على نطاق واسع في المؤسسة لكافة المستويات ، وتحدثت في محورها الرابع عن آلية التعامل مع الحوادث من خلال استعادة البيانات و خطة إدارة الحادث والمراحل التي تمر بها فرق الاستجابة اثناء الحوادث وضرورة إعداد التقارير وماذا يجب أن تحتوي هذه التقارير وكيفية صياغتها وكذلك عملية اختبار الاستجابة للحادث والدروس المستفادة من عملية تحليل الحادث، وتحدثت في محورها الخامس عن إدارة استمرارية العمل وأنه لابد من وضع خطة لاستمرارية العمل والتقليل من أثر الحادث ولابد لتطبيق ذلك من مجموعة نقاط وهي التزام الإدارة ووضع برنامج لدورة إدارة استمرارية العمل وتقييم إدارة استمرارية العمل والذي يتضمن تقييم الأداء و المراقبة والقياس والتحليل والتقييم ومن ثم التدقيق الداخلي ومراجعة الإدارة والتواصل مع الأطراف المعنية وتحديد أهم المعايير لإجراء هذه الخطوات وفي محورها السادس تحدثت عن أهم الاعتبارات الأساسية من أجل الاستجابة لدى وقوع حادث.

---

[72] **المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 6 (ب) سياسة الاستجابة لدى وقوع حادث.**

(ج): التحسين المستمر، الدروس المستفادة، والمراجعات، والتحسين المستمر(2):[73] وتكونت هذه الوثيقة من (10) صفحات و (4) محاور أساسية تضمنت في محورها الأول الهدف التي تم انشاؤها من أجله وبيان انها وثيقة ليست مستقلة دون باقي السياسات، وبيان المتطلبات الأساسية ، وتبين أنها تنطبق على جميع موظفي الحكومة الأردنية، وتطرقت إلى المعايير والأطر الدولية التي تمت الاستعانة بها مثل: (ISO 9000)، و (ISO 9001) و (ISO 9004) و (ISO 19011) ، وتحدثت في محورها الثاني عن تطبيق التحسين المستمر وتحديد فرص تحسين الأداء ومشاركة أفضل الممارسات وبينت الهدف من التحسين المستمر وأهم المبادئ الأساسية للتحسين المستمر وأنه لابد للإدارة العليا من التواصل مع المعنيين ودعم كل ما يتعلق بالتحسين المستمر ويتم ذلك أيضا من خلال التدريب والتعليم، وتحدثت في شقها الثالث عن طرق التحسين المستمر وذكرت أحد النماذج لذلك وهو نموذج التخطيط والفعل والتحقق واتخاذ الإجراء ووضحت كل واحدة من هذه العمليات وكيفية اتمامها على أفضل وجه ، ومن ثم انتقلت للتحدث عن تحليل أسباب المشكلة والتعلم من التجربة، وتحدثت في محورها الرابع عن أهم الاعتبارات الأساسية من أجل تطبيق هذه السياسة.

الخاتمة

في السنوات القليلة الماضية زاد الانفتاح على الأمن السيبراني في المملكة الأردنية الهاشمية بعد انتشار هذا المصطلح وازدياد حالات عمليات الاختراقات الإلكترونية والهجمات السيبرانية ومن أهم الفئات التي ازداد فيها الاهتمام بالأمن السيبراني الدوائر الحكومية وذلك بعد نشر سياسات الأمن السيبراني التي يعنى بها كل موظف في القطاع العام ،وكذلك تك عقد العديد من المؤتمرات والندوات حول الموضوع ، وقامت العديد من الجامعات الحكومية والخاصة بفتح تخصص الأمن السيبراني مثل جامعة اليرموك وجامعة البلقاء التطبيقية وجامعة الأميرة سمية للتكنولوجيا وجامعة فيلادلفيا وتم انشاء العديد من المختبرات الخاصة بالأمن السيبراني في الجامعات مثل جامعة العلوم والتكنولوجيا و_*جامعة* عمان الأهلية وجامعة الزيتونة وغيرها وتم تشجيع الطلاب والدارسين للدخول في هذا المجال وبيان أهميته ومدى استيعاب سوق العمل وافتقاره للوظائف التي تتعلق بهذا التخصص ، وازداد انتشار الأبحاث العلمية بهذا المجال وكذلك توسع هذا الانتشار ليشمل الشركات

[73] **المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 6 (ج) سياسة التحسين المستمر.**

الخاصة وسوق العمل بحيث أصبح هنالك العديد من الشركات العاملة في هذا المجال وازدادت فرص العمل المتعلقة به وكذلك ازداد عدد مراكز التدريب التي تعنى بالتدريب على مهارات الأمن السيبراني المختلفة .

ويرى الباحث كما تم توضيحه سابقا أن قانون الأمن السيبراني في عنوانه جاء بمخالفة نص قانون أخر تم اقراره سابقا حيث نصت المادة (11) من قانون حماية اللغة العربية رقم 35 لعام 2015 "تصاغ جميع تشريعات الدولة باللغة العربية" وبما أن كلمة (السيبراني) ليست كلمة عربية فإن عنوان قانون الأمن السيبراني وبعض المواد التي يتضمنها كانت مخالفة واضحة لأحد القوانين الأردنية المنشورة سابقا.

ويرى الباحث أن من أهم ما افتقرت إليه التشريعات والاستراتيجيات والسياسات نشر أنظمة تبين الإجراءات التي سيتم تطبيقها على أرض الواقع خصوصا كون هذه التشريعات والاستراتيجيات والسياسات تحدثت عن شمول كافة مؤسسات الدولة بها دون فعلية لابد من اصدار أنظمة تبين كافة الإجراءات الفنية والميدانية المتعلقة بعمل المجلس مع كافة مؤسسات الدولة وكافة أفرادها بما يخص الأمن السيبراني والتي نتطلع إلى رؤيتها في الفترة القادمة إن شاء الله.

ويتطلع الباحث إلى نشر قوانين وأنظمة متعلقة بآليات تطبيق سياسات الأمن السيبراني وأن تحتوي على إجراءات ميدانية للعمل بها وعلى عقوبات واضحة كون القانون الحالي تنظيمي وأن يتم التوصل إلى صياغة تتماشى مع كافة القوانين النافذة في المملكة الأردنية الهاشمية.

- ج. صليبا، المعجم الفلسفي، .volالجزء الأول صفحة 682, بيروت: دار الكتاب اللبناني, 2008.
- م. البعلبكي، السِّيبَرناتية؛ علم الضبط؛ موسوعة المورد صفحة 307, بيروت: دار العلم للملايين, 1991.
- المملكة الأردنية الهاشمية، رئاسة الوزراء، قانــون رقم (16) لسنة 2019 - قانون الأمن السيبرانــي، عمان، الأردن: رئاسة الوزراء، الجريدة الرسمية عدد 5595, 2019.
- المملكة الأردنية الهاشمية، رئاسة الوزراء، "السياسة العامة للحكومة في قطاعات الاتصالات وتكنولوجيا المعلومات والبريد 2007," وزارة الاتصالات وتكنولوجيا المعلومات، 2007
- [Online]. Available:
- trc.gov.jo/EchoBusV3.0/SystemAssets/202007%لعام20%السياسة20%وثيقة.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "السياسات الوطنية لأمن وحماية المعلومات،" 2008
- . [Online]. Available: www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/
- السياسات_الوطنية_لأمن_وحماية_المعلومات_2008.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "الاستراتيجية الوطنية لضمان امن المعلومات وامن الفضاء السيبراني،" مركز تكنولوجيا المعلومات الوطني,
- 2012 . [Online]. Available
- trc.gov.jo/EchoBusV3.0/SystemAssets/20%المعلومات20%امن20%لضمان20%الوطنية20%الإستراتيجية 202012%20%السيبراني20%والأمن.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "وثيقة السياسة العامة للحكومة في قطاعات الاتصالات وتكنولوجيا المعلومات والبريد للعام،" 2012
- [Online]. Available:
- trc.gov.jo/EchoBusV3.0/SystemAssets/202012%لعام20%السياسة20%وثيقة.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "الاستراتيجية الوطنية للأم_السيبراني 2018 - 2023," 2018
- . [Online]. Available:
- www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/20_الاستراتيجية_الوطنية_للأمن_السيبراني 2023_18.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "السياسة العامة لقطاعات الاتصالات وتكنولوجيا المعلومات والبريد 2018," 2018

- [Online]. Available:
- trc.gov.jo/EchoBusV3.0/SystemAssets/About%20TRC/014da924b8084372b2a961a49d19e5eb_ICTP_Policy_2018.pdf.
- المملكة الأردنية الهاشمية، رئاسة الوزراء، قانون رقم (35) لسنة 2015- قـانون حماية اللغـة العربيـــة، عمان، الأردن: رئاسة الوزراء، الجريدة الرسمية عدد 5347، 2015 .
- المملكة الأردنية الهاشمية، رئاسة الوزراء، نظام رقم (1) لسنة 2020 -نظام المركز الوطني للأمن السيبراني، عمان، الأردن: رئاسة الوزراء، الجريدة الرسمية عدد 5614, 2020.
- المملكة الأردنية الهاشمية، رئاسة الوزراء، نظام رقم (25) لسنة 2021 - نظام التنظيم الإداري للمركز الوطني للأمن السيبراني، عمان، الأردن: رئاسة الوزراء، الجريدة الرسمية عدد 5721, 2021.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 1 (أ) الأدوار والمسائلة والمسؤوليات، " [Online]. Available: www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_الأدوار_والمساءلة_والمسؤوليات.pdf .
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 1 (ب) سياسة إدارة المخاطر، " [Online]. Available: www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_إدارة_المخاطر.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 1 (ج) سياسة التدقيق والضمان، " [Online]. Available: www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_التدقيق_والضمان.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 1 (د) سياسة الامتثال الدولي، " [Online]. Available: www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_الامتثال_الدولي.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 2 (أ) سياسة نظام العلامات الوقائية، " [Online]. Available: www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_نظام_العلامات_الوقائية.pdf.

- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 2 (ب) سياسة الحماية والإفصاح ",[Online]. Available: www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_الحماية_والإفصاح.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 2 (ج) إدارة الموارد ",[Online]. Available: www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_إدارة_الموارد.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 3 (أ) سياسة معايير أمن الأفراد ",[Online]. Available: www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_معايير_أمن_الأفراد.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 6 (ب) سياسة التصريح الأمني ",[Online]. Available: www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_التصريح_الأمني.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 4 (أ) سياسة أمن المعلومات، "[Online]. Available: www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_أمن_المعلومات.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 4 (ب) سياسة ضمان المعلومات، "[Online]. Available: www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_ضمان_المعلومات.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 4 (ج) إدارة توليف الشبكة ",[Online]. Available: www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_إدارة_توليف_الشبكات.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 4 (د) سياسة الأجهزة المحمولة ",[Online]. Available: www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_الأجهزة_المحمولة.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 4 (هـ) سياسة المراقبة الوقائية ",[Online]. Available: www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_المراقبة_الوقائية.pdf.

- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 5 (أ) سياسة الوسائل الدفاعية المتعمقة: Available: [Online]. ," www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_الوسائل_الدفاعية_المتعمقة.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 5 (ب) سياسة الحاويات والتخزين: Available: [Online]. ," www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_الحاويات_والتخزين.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 5 (ج) سياسة الدخول إلى الموقع: Available: [Online]. ," www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_الدخول_الى_الموقع.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "لبرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 6 (أ) إدارة التغيير: Available: [Online]. ," www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_إدارة_التغيير.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 6 (ب) سياسة الاستجابة لدى وقوع حادث: Available: [Online]. ," www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_الاستجابة_لدى_وقوع_حادث.pdf.
- المملكة الأردنية الهاشمية، وزارة الاتصالات وتكنولوجيا المعلومات، "البرنامج الوطني للأمن السيبراني إطار سياسة الأمن السيبراني 6 (ج) سياسة التحسين المستمر," Available: [Online]. www.modee.gov.jo/ebv4.0/root_storage/ar/eb_list_page/سياسة_التحسين_المستمر.pdf.

استراتيجيات الأمن السيبراني في المغرب من خلال القانون 05.20

الأستاذ عمر اللطيفي
مستشار بمحكمة الاستئناف بمراكش، وعضو
الودادية الودادية الحسنية للقضاة (المغرب)

تقديم

لعل التوجه إلى الرقمنة والعمل الذكي والالكتروني المعتمد أساسا على خدمات الانترنت والوسائط الالكترونية الذي أصبح واقعا فارضا لنفسه على مؤسسات الدولة وإدارتها وجماعاتها الترابية و قطاعها الخاص من شركات ومقاولات ، بل وحتى على الأفراد ، حتم ضرورة تعزيز و تقوية الثقة الرقمية والاطمئنان إلى سلامة وأمن نظم المعلومات والخدمات المقدمة بواسطة هذه التقنيات وداخل هذه البيئة الجديدة أو ما سمي بالفضاء السيبراني اللامادي ، والتحول الى الايمان بجدوى هذه الخدمات وأهميتها وما توفره من فوائد جمة لبني البشر .

فتأمين نظم المعلومات أو ما يصطلح عليه بالأمن السيبراني يعد الهاجس الذي يتملك كل الأنظمة، والدول تسعى إلى تحقيقه بكل الآليات المتوفرة والممكنة. ولعل آلية التشريع و وضع الضوابط القانونية و المؤسساتية بالقانون لتحقيق أمن نظم المعلومات يعد حجر الزاوية والعمود الفقري الذي تتأسس عليه الحماية المنشودة .

و في هذا السياق بدأ المغرب خاصة مع نهاية القرن الماضي يؤسس لترسانة تشريعية رقمية تستهدف تحقيق تحول رقمي آمن من خلال مجموعة من القوانين التي تدرجت في الأخذ بأحدث المقتضيات التشريعية والمؤسساتية العالمية وتكاملية يراعى فيها التوجه العالمي في هذا الباب ومحاولة مجاراة إيقاع هذا التوجه والانخراط فيه وتنزيل مقتضياته وطنيا ، إذ تشكل المصادقة على العديد من الاتفاقيات الدولية وإقرارها في القانون الداخلي مظهرا من مظاهر هذا التكامل والتعاون الدولي الذي لا مناص منه في ظل البيئة الرقمية التي لا تؤمن بالحدود وتعدد المخاطر والتهديدات السيبرانية ذات المصادر و المنابع المتعددة مع رسم اهداف ووضع استراتيجيات وإنشاء هيئات لتنزيلها .

وفي إطار هذه الحركية التشريعية وفي سبيل تحقيق أمن سيبراني وتعزيز خدمات الثقة في المعاملات الإلكترونية صدر القانون 20. 05بتاريخ 25 يوليوز 2020 ونشر بالجريدة الرسمية عدد 6904 بتاريخ 30 يوليوز 2020 من أجل حماية نظم معلومات إدارات الدولة و الجماعات الترابية والمؤسسات والمقاولات العمومية وكل شخص اعتباري آخر خاضع للقانون العام ، والتي أشار اليها المشرع بلفظ (الهيئة)ووضع قواعد ومقتضيات الأمن المطبقة على البنيات التحتية ذات الأهمية الحيوية وقواعد ومقتضيات الأمن المطبقة على مستغلي الشبكات العامة للمواصلات ومزودي خدمة الانترنت ومقدمي خدمات الأمن السيبراني ، والخدمات الرقمية وهو ما أشار إليه القانون بتسمية (المتعهد) .

مع تحديد الاطار الوطني لحكامة الأمن السيبراني وتعزيز التعاون بين السلطة الوطنـية ، مع تحديد المساهمات التي تقدمها السلطة الوطنية لتعزيز الثقـة الرقمية وتطوير الخدمات المقـدمة من طرف الدولة ،وكذا تحديد اختصاصات السلطة الوطنية و ما يتعلق بتطوير الخبرة الوطنيـة والتحسيس في مجال الأمن السيبراني لفائدة الهيئات والفاعليـن في القطاع الخاص والأفراد وتقوية التعاون مع المؤسسات الوطنية و الأجنبية.

وإذا كانت هذه هي الخطوط العريضة التي حاول القانون الاشتغال عليها وتناولها من خلال 53 فصلا فإنه يصعب ايراد مقتضياتها كاملة في مجرد هذه الورقة ،لذلك فإني آثرت أن اتداول اشكالا يتيره الموضوع متصلا اتصالا جذريا بعنوان المداخلة وهو كالآتي:

- ما هي الأهداف والهيئات التي أتى بها هذا القانون 05.20 والتي تكرس لنا استراتيجيات الأمن السيبراني في المغرب من خلاله ؟

وتحليل هذا الإشكال سوف نتطرق إليه من خلال نقطتين أساسيتين :

- أولا الأهداف التي ترمي إلى تحقيقها استراتيجيات الأمن السيبراني في القانون 05.20
- ثانيا: الهيئات الداعمة لتنفيذ استراتيجيات الأمن السيبراني في إطار القانون 20.05

المطلب الاول: الأهداف التي ترمي الى تحقيقها استراتيجيات الأمن السيبراني في القانون20.05

تتجلى أهم الأهداف التي يرمي إلى تحقيقها القانون من خلال الدراسة المتأنية لمواده وكدا من خلال الاطلاع على النقاشات التي سبقت إقراره بقبة البرلمان[74] في ما يلي :

1. تعزيز حماية وصمود نظم المعلومات :

تتجلى الأهداف الأساسية لهذا القانون في وضع قواعد قانونية بشأن وسائل الحماية الرامية إلى تعزيز الثقة ودعم الاقتصاد الرقمي ، وبشكل أعم ضمان استمرارية الأنشطة الاقتصادية والاجتماعية لبلادنا.

ولهذا الغرض ولتحقيق الأهداف الإستراتيجية الوطنية للأمن السيبراني ، لا سيما التي تهم تعزيز حماية وصمود نظم معلومات الدولة والجماعات الترابية وكذا البنيات

التحتية ذات الأهمية الحيوية ، يتضمن القانون تدابير أمنية تهدف إلى تقوية القدرات الوطنية في هذا المجال والمساهمة في تأهيل عملية التحول الرقمي بالمغرب وكذا تنسيق إجراءات الوقاية والحماية في مواجهة هجمات وحوادث الأمن السيبراني .

وفي هذا الصدد ، يرمي القانون إلى وضع إطار قانوني يلزم إدارات الدولة والجماعات الترابية والمؤسسات و المقاولات العمومية و كل شخص اعتباري آخر خاضع للقانون العام ، المشار إليهم فيما بعد بالهيئات ، باحترام التوجيهات والقواعد والأنظمة والمراجع والتوصيات الصادرة عن السلطة الوطنية في هذا المجال.

كما يفرض هذا القانون على هذه الهيئات تنفيذ التدابير التقنية والتنظيمية لإدارة المخاطر السيبرانية وتجنب الحوادث التي قد تؤثر على نظم المعلومات والالتزام بإبلاغ السلطة الوطنية للأمن السيبراني بأي حادث يؤثر على أمن أو نظم المعلومات الخاصة بها و ذلك حتى يتسنى للسلطة الوطنية إيجاد الحلول الناجعة من أجل تجاوز هذه الحوادث.

---

[74] -يراجع تقرير لجنة الخارجية والدفاع الوطني والشؤون الإسلامية والمعارضة المقيمين بالخارج حول مشروع قانون رقم 20/05 يتعلق بالامن السبراني ، مجلس النواب ، دورة ابريل 2020.

ويلزم هذا القانون كل هيئة بتعيين مسؤول عن أمن نظم المعلومات وإعداد مخططات ضمان استمرارية واستئناف الأنشطة في أقرب الآجال لإبطال مفعول انقطاعها.

وبالإضافة إلى الإجراءات الأمنية التي تخضع لها تلك الهيئات والتي تسري أيضا على البنيات التحتية ذات الأهمية الحيوية ، ينص القانون على أحكام إضافية خاصة بالبنيات التحتية ذات الأهمية الحيوية التي تتوفر على نظم معلومات حساسة، لا سيما تلك المتعلقة بالمصادقة على نظم المعلومات الحساسة الخاصة بها ، و إخضاع هذه النظم لافتحاصات أمنية وإلزامهما بالإيواء الحصري لمعطياتها الحساسة داخل التراب الوطني.

2- توسيع نطاق الحماية بدمج فئات فاعلة أخرى.

ينص قانون الأمن السيبراني على اتخاذ التدابير التقنية والتنظيمية اللازمة المساهمة في حماية شبكات ونظم معلومات فئات فاعلة أخرى تشمل مستغلي الشبكات العامة للمواصلات ، ومزودي خدمات الانترنيت ، ومقدمي خدمات الأمن السيبراني ، ومقدمي الخدمات الرقمية وناشري منصات الانترنيت.

وبالنظر للدور الاستراتيجي الذي يلعبه هؤلاء المتعهدون في تعزيز أمن نظم معلومات الهيئات والبنيات التحتية ذات الأهمية الحيوية ومتعهدي القطاع الخاص والأفراد ، فقد نص القانون كذلك على ضرورة احتفاظهم بالمعطيات التقنية الكفيلة بتحديد حوادث الأمن السيبراني و التي تتضمن على الخصوص ، بيانات الربط والنشرات المعلوماتية وآثار أحداث الأمن المحصل عليها بواسطة نظم الاستغلال والتطبيقات ومنتوجات الأمن وكذلك الإبلاغ عن أي حادث قد يؤثر على أمن نظم معلومات زبنائهم واتخاذ التدابير الوقائية اللازمة لمنع وتخفيف وقع التهديدات أو المساس بهذه النظم .

كما يولي القانون كذلك أهمية كبيرة للوقاية والتحسيس بشأن تحديات الأمن السيبراني ، حيث يعيد للسلطة الوطنية بأن تنشر بانتظام على موقعها الالكتروني النصائح والتوصيات الوقائية المتعلقة بالأمن السيبراني لفائدة إدارات الدولة والجماعات الترابية والمؤسسات والمقاولات العمومية والبنيات التحتية ذات الأهمية الحيوية ومتعهدي القطاع الخاص والمواطنين.

3- مواجهة الهجمات السيبرانية وتعزيز الرقمنة وحماية المعطيات الشخصية والحساسة

يشكل تبادل المعلومات و المعطيات بين المصالح المختصة للدولة محورا أساسيا وهاما في مكافحة الهجمات السيبرانية . ولأجل ذلك ، يضع القانون إطارا للتعاون وتبادل المعلومات بين السلطة الوطنية للأمن

السيبراني والمصالح المختصة في الدولة المكلفة بالتصدي للجرائم التي تخل بسير نظم المعالجة الآلية للمعطيات.

كما تسهم السلطة الوطنية وفقا لهذا القانون ، في دعم البرامج التي تعدها الهيئات المختصة في الدولة من أجل تعزيز الثقة وتطوير رقمنة الخدمات وحماية المعطيات ذات الطابع الشخصي . وفي هذا الإطار وجب التذكير بالدور المهم الذي قامت و تقوم به المديرية العامة لأمن نظم المعلومات في ظل الظروف الاستثنائية التي تعيشها بلادنا) و باء كوفيد 19 (حيث تم استصدار مذكرة حول الأمن السيبراني تتعلق بالعمل عن بعد و التي حددت المعايير الواجب الالتزام بها عند استخدام مختلف الوسائل التقنية كا فتحاص المنصات و الأنظمة المعلوماتية قبل توجيهها للعمل عن بعد وتجنب تقاسم المعلومات الحساسة خلال اجتماعات و جلسات الفيديو (visioconférence) وعدم تثبيت التطبيقات الغير الموثوقة المصدر و البرامج الخبيثة على الحاسوب أو الهاتف المحمول والالتزام بتوجيهات المسؤولين عن نظم المعلومات و أمنها بالإضافة إلى اخطارهم بأي طارئ أو حادث يهم أمن نظم المعلومات .

وقد تم العمل بهده التقنية في محاكم المملكة خلال اعلان حالة الطوارئ الصحية ولازال الامر قائما في قضايا المعتقلين احتياطيا ضمان لاستمرار خدمات العدالة باعتبارها من القطاعات الحيوية التي يصعب توقف خدماتها وقد تم تامين التقنية بالتزام من وزارة العدل وشركائها حفاظا على حقوق الدفاع واحتراما للخصوصية ومبادئ المحاكمة العادلة.

ومن أجل مضاعفة قدرات التصدي للهجمات السيبرانية ، فإن مشروع القانون يعطي أولوية هامة لتنمية التعاون و تطوير تبادل التجارب والخبرات مع المنظمات والمؤسسات الأجنبية المماثلة. وفي هذا الإطار ، فقد تم إبرام العديد من اتفاقيات التعاون و التبادل التي تهدف إلى تشجيع الرفع من القدرات و ملاءمة الجهاز التنظيمي و التشريعي في مجال الأمن السيبراني و تنمية تبادل الخبرات بين المركز المغربي لليقظة و الرصد والتصدي للهجمات المعلوماتية التابع للمدير العامة لأمن نظم المعلومات و نظرائه في الخارج من خلال تبادل المعلومات العلمانية التي تساهم في معالجة الحوادث المتعلقة بأم طم المعلومات و تبادل تقارير التحاليل و الخبرات و المشورة بشأن قضايا الأمن السيبراني بالإضافة إلى نقل الخبرات في مجال تحليل البرامج الخبيثة و تقييم أنظمة حماية نطم المعلومات.

4- تخويل اللجنة الاستراتيجية و السلطة الوطنية صلاحيات ووسائل الاضطلاع بمهمة حماية نظم المعلومات

يولي هذا القانون أهمية بالغة لحكامة الأمن السيبراني من خلال تحديد المهام الموكلة إلى اللجنة الاستراتيجية للأمن السيبراني والسلطة الوطنية للأمن السيبراني ، كما ينص القانون على إمكانية إجراء عمليات افتحاص وحماية نظم المعلومات . وتتم عمليات الافتحاص من قبل الأعوان المعتمدين من طرف السلطة الوطنية أو من قبل متعهدي الافتحاص المؤهلين من طرف السلطة الوطنية.

و في هذا الصدد و سعيا منها لتطوير القدرات اللازمة لحماية المصالح الحيوية للدولة والاقتصاد الوطني في مجال أمن نظم المعلومات، قامت المديرية العامة بفضل كفاءاتها الداخلية على مدى السنوات الماضية بتدقيق وافتحاص أمن نظم معلومات بعض الوزارات والمؤسسات العمومية والهيئات ذات الطابع الاستراتيجي ، وقد ساهمت التوصيات التي أصدرتها المديرية عقب هذه العمليات في تحسيس هذه الهيئات حول ضرورة تطبيق بعض الإجراءات الاحترازية من أجل تأمين أفضل لسلامة أمن نظم معلوماتها.

5- تعزيز وتطوير البيئة الوطنية للأمن السيبراني

إضافة إلى التأثير المباشر على تأمين سير الاقتصاد والمجتمع ، سيما وأن هذا القانون جاء من أجل تعزيز البيئة الوطنية للأمن السيبراني ، وهو ما سيعطي دفعة لتطوير الخدمات في مجال الاستشارة والافتحاص والرصد ومعالجة حوادث الأمن السيبراني وكذا المنتوجات التي تسمح بتأمين الشبكات ونظم المعلومات وتعزيز خدمات الثقة بشأن المعاملات الالكترونية.

ولضمان تطبيق وتنفيذ أحكام هذا القانون ، يتضمن هذا النص مقتضيات زجرية في حالة الإخلال ، مثل عدم الإبلاغ عن الحوادث التي تؤثر على نظم المعلومات ، أو إيواء المعطيات الحساسة خارج التراب الوطني ، أو إعاقة إجراء عمليات افتحاص أمن نظم المعلومات ، أو عدم تنفيذ القرارات والتدابير الأمنية الصادرة عن السلطة الوطنية للأمن السيبراني.

المطلب الثاني : الهيئات الداعمة لتنفيذ استراتيجيات الأمن السيبراني في القانون 20.05

لقد أحدث المشرع المغربي بمقتضى المادة 35 من القانون 05.20 لجنة استراتيجية للأمن السيبراني والتي أوكل اليها تنزيل سياسة المغرب واستراتيجياته في مجال الأمن السيبراني، وسنتحدث عن تأليف و كيفيات سير أعمال هذه اللجنة

الفقرة الاولى : اللجنة الاستراتيجية للامن السبراني(التأليف والمهام) .

1: تأليف اللجنة الاستراتيجية للأمن السيبراني

كلنا يعلم أن المشرع المغربي أصدر القانون 20.05 المتعلق بالأمن السيبراني و هو عبارة عن مجموعة من التدابير والإجراءات ومفاهيم الأمن وطرق إدارة المخاطر والأعمال والتكوينات وأفضل الممارسات التي تسمح لنظام معلومات أن يقاوم أحداثا مرتبطة بالفضاء

السيبراني . وقد كلف المشرع بتنزيل مقتضيات هذا القانون للجنة الاستراتيجية للأمن والتي تتألف من مجموعة من الأشخاص حسب المادة 2 من المرسوم التطبيقي لقانون 05.20[75]، ويترأس اللجنة الاستراتيجية للأمن السيبراني المنصوص عليها في المادة 35 من القانون السالف الذكر ،الوزير المنتدب لدى رئيس الحكومة المكلف بإدارة الدفاع الوطني، وتتألف من مجموعة من الأعضاء الساميين في الدولة كما جاء في المادة

2: مهام اللجنة الاستراتيجية للأمن السيبراني

لقد حدد المشرع المغربي مهام اللجنة الاستراتيجية للأمن السيبراني بمقتضى المادة 35 من القانون 20.05 وهي كالآتي:

- إعداد التوجهات الإستراتيجية للدولة في مجال الأمن السيبراني والسهر على ضمان صمود نظم معلومات الهيئات والبنيات التحتية ذات الأهمية الحيوية و المتعهدين المشار إليهم في الفرع الثالث من الفصل الثاني من هذا القانون.
- التقييم السنوي لأنشطة السلطة الوطنية.
- تقيم عمل اللجنة الوطنية لإدارة الأزمات والأحداث السيبرانية الجسيمة المنصوص عليها بمقتضى المادة 36 من القانون 20.05.
- -حصر نطاق افتحاصات نظم المعلومات التي تنجزها السلطة الوطنية.
- تشجيع البحث والتطوير في مجال الأمن السيبراني.
- تشجيع برامج وأنشطة التحسيس وتعزيز القدرات في مجال الأمن السيبراني لفائدة الهيئات والبنيات التحتية ذات الأهمية الحيوية.
- إبداء الرأي في مشاريع القوانين و النصوص التنظيمية المتعلقة بمجال الأمن السيبراني .

---

[75] -المرسوم رقم 2.21.406 الصادر في 4 ذي الحجة 1442 (20 يوليو 2021)، الجريدة الرسمية عدد 7011، ذو الحجة 1442 (9 أغسطس 2021) ص، 5979، والقاضي بتطبيق القانون رقم 05.20 المتعلق بالأمن السيبراني

ولدى هذه اللجنة الاستراتيجية للأمن السيبراني تحدث لجنة خاصة لإدارة الأزمات والأحداث السيبرانية الجسيمة وهي محور المطلب الثاني من هذا المبحث.

الفقرة الثانية: لجنة إدارة الأزمات والأحداث السيبرانية الجسيمة (التأليف والاختصاصات) .

لقد خصصنا الحديث في هذا الفقرة عن تأليف لجنة إدارة الأزمات و الأحداث السيبرانية الجسيمة **(اولا)** في حين سنتحدث على مهام هذه اللجنة **(ثانيا)** .

1: تأليف لجنة إدارة الأزمات و الأحداث السيبرانية الجسيمة

كما سبق أن تحدثنا في الفقرة اعلاه، فالقانون السيبراني يتضمن قواعد ومقتضيات الأمن المطبقة على نظم معلومات إدارة الدولة والجماعات الترابية والمؤسسات والمقاولات العمومية و ذلك في إطار التعاون و تبادل المعلومات بين السلطة الوطنية للأمن السيبراني و المصالح

المختصة للدولة المكلفة بمعالجة الجرائم الماسة بنظم المعالجة الآلية للمعطيات , ومن أجل هذا كلف المشرع المغربي بتنزيل هذه المقتضيات على أرض الواقع لجنة استراتيجية تحدث لديها لجنة خاصة بإدارة الأزمات و الأحداث السيبرانية الجسيمة والتي تتألف بمقتضى المادة 6 من المرسوم التطبيقي لقانون 05.20 من مجموعة من السلطات وتترأسها المديرية العامة لأمن نظم المعلومات.

2: مهام لجنة إدارة الأزمات والأحداث السيبرانية الجسيمة

بعودتنا إلى مقتضيات المادة 36 من القانون السيبراني نجدها تنص على أن لجنة إدارة الأزمات و الأحدا ث السيبرانية الجسيمة تتكلف بضمان تدخل منسق في مجال الوقاية وتدبير الأزمات على اثر وقوع حوادث امن سيبراني , ولهذا الغرض يتعين على مستغلي الشبكات العامة للمواصلات ومزودي خدمات الانترنيت ومقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية الامتثال للأوامر الصادرة عن لجنة إدارة الأزمات و الأحداث السيبرانية الجسيمة و الاستجابة لطلباتها المتعلقة بالدعم والمساعدة التقنية.

الفقرة الثالثة : السلطة الوطنية للأمن السيبراني

في ظل التوجه الدولي للحد من التهديدات السيبرانية أصبحت قضية الأمن السيبراني من التحديات الكبرى على الصعيدين الإقليمي والعالمي ، والمغرب بدوره يسعى الى حماية منظومته المعلوماتية من خلال العديد من الأجهزة ، التي من بينها السلطة الوطنية موضوع الدراسة في هذا البحث حيث سنتناول مهام السلطة

الوطنية للأمن السيبراني وذلك من خلال الحديث على تنفيذ استراتيجية الدولة في مجال الأمن السيبراني، ثم دور السلطة الوطنية في التعاون و التحسيس و معاينة المخالفات و العقوبات وذلك في المطلب الثالث.

المطلب الثالث : تنفيذ إستراتيجية الدولة في مجال الأمن السيبراني

سنقسم هذا المطلب إلى قسمين حيث سنتطرق لمهمة تنفيذ إستراتيجية الدولة من جهتين, من حيث تنفيذ إستراتيجية الدولة في مجال الأمن السيبراني من جهة (الفقرة الأولى) , ثم من حيث تحديد قواعد الأمن اللازمة لحماية نظم المعلومات والتصدي للهجومات الالكترونية التي تستهدفها من جهة ثانية (الفقرة الثانية).

الفقرة الأولى : من حيث تنفيذ إستراتيجية الدولة في مجال الأمن السيبراني

بقراءتنا لمقتضيات المادة 38 من القانون السيبراني نجدها تنص على أنه بالإضافة إلى تنفيذ إستراتيجية الدولة في مجال الأمن السيبراني المسندة إلى السلطة الوطنية للأمن السيبراني فإن هذه الأخيرة تقوم بالمهام التالية :

- تنسيق الأعمال المتعلقة بإعداد وتنفيذ إستراتيجية الدولة في مجال الأمن السيبراني والسهر على ضمان تطبيق توجيهات اللجنة الاستراتيجية للأمن السيبراني.
- تحديد تدابير نظم المعلومات و السهر على ضمان تطبيقها.
- تقديم اقتراحات إلى اللجنة الاستراتيجية للأمن السيبراني بخصوص تدابير التصدي اللازمات التي تمس او هدد امن نظم معلومات الهيئات و البنيات التحتية ذات الأهمية الحيوية.
- تأهيل مقدمي خدمات افتحاص نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية ومقدمي خدمات الأمن السيبراني.
- وضع تصور للوسائل اللازمة لضمان أمن الاتصالات الالكترونية بين الوزارية وتنسيق تفعيلها .
- القيام بأعمال المراقبة المنصوص عليها في القانون 20.05 .
- السهر على ضمان إجراء عمليات افتحاص نظم معلومات الهيئات و البنيات التحتية ذات الأهمية الحيوية
- افتحاص متعهدي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية الذين يقدمون خدمات البنيات التحتية ذات الأهمية الحيوية المتوفرة على نظم معلومات حساسة.

- تقديم المساعدة و النصائح إلى الهيئات و البنيات التحتية ذات الأهمية الحيوية قصد تعزيز أمن نظم معلوماتها .
- مساعدة ومواكبة الهيئات و البنيات التحتية ذات الأهمية الحيوية لوضع أجهزة الرصد احداث سمت أو قد تمس بأمن نظم معلوماتها وكذا تنسيق إجراءات التصدي لهذه الأحداث .
- القيام بأنشطة البحث العلمي و التقني في مجال الأمن السيبراني وتشجيعها.
- هذا ويتعين على السلطة الوطنية ضمان سرية المعلومات الحساسة التي تجمعها في اطار القانون 20.05 .

الفقرة الثانية: من حيث تحديد قواعد الأمن اللازمة لحماية نظم المعلومات و التصدي للهجمات الإلكترونية التي تستهدفها

إلى جانب قيام السلطة الوطنية بالمهام السالفة الذكر اعلاه و بالعودة إلى مقتضيات المادة 40 من القانون السيبراني نجدها تنص على أن السلطة الوطنية تحدد قواعد الأمن اللازمة لحماية نظم معلومات الهيئات والبنيات التحتية ذات الأهمية الحيوية , كما تحدد قواعد امن خاصة بقطاع أنشطة ذي أهمية حيوية، وتقوم بتبليغ هذه القواعد وكذا كيفيات واجل تطبيقها إلى مسؤولي البنيات التحتية ذات الأهمية الحيوية التابعين للقطاع المعني.

هذا ولأجل التصدي لأي هجوم الكتروني يستهدف نظم المعلومات ويمس بالوظائف الحيوية للمجتمع أو الصحة أو السلامة أو الأمن أو التقدم الاقتصادي أو الاجتماعي ، يقوم أعوان السلطة الوطنية بالتحريات التقنية اللازمة لتحديد خصائص الهجوم ويسهرون على

ضمان تنفيذ التدابير و التوصيات المتعلقة، ونجد المادة 41 تنص على أنه تتعاون السلطة الوطنية مع المصالح المختصة في الدولة من خلال تبادل أي معطيات أو معلومات قد تساعدها على معالجة الجرائم التي تخل بسير نظم المعالجة الآلية للمعطيات وذلك في حالة تبين للسلطة الوطنية أثناء ممارستها لمهامها وجود فعل يشتبه في مخالفته.

خصوصية جريمة الإرهاب السيبراني وآليات مواجهته

الدكتور محمد الايوبي
أستاذ باحث بالكلية المتعددة التخصصات بالرشيدية
جامعة المولي إسماعيل (المغرب)

ملخص

لقد أحدث تطور المعلومات والاتصالات ثورة شاملة في جميع نواحي الحياة، وهو ما شكل إيذانا ببروز بيئة جديدة للتفاعل بين الأفراد والمجتمعات والدول، اصطلح على تسميتها بالفضاء السيبراني، هذا الفضاء الذي يتميز بالتطور السريع، والغموض الشديد، قد ساهم بطرق مختلفة وأساليب متعددة- منها المعقدة والسهلة - في تطور أشكال الإجرام على كافة المستويات الاجتماعية والاقتصادية والثقافية والسياسية....

ومما عزز خطورة هذه التكنولوجيا، كونها عابرة للحدود الوطنية وانتشار شبكاتها عالميا، إذ لا تقتصر تهديدات الفضاء الالكتروني على المستوى الوطني، بل تتعداه اليوم إلى تهديدات أمن وسلامة الدول.

وإن من أهم الجرائم التي تشكل الفضاء السيبراني إضافة ومنعرجا حاسما بالنسبة لها هي الإرهاب السيبراني، باعتباره من الجرائم التي تنعكس آثارها على المستويين الوطني والدولي.

لذلك تناقش هذه الورقة البحثية خصوصية وطبيعة مفهوم "الإرهاب السيبراني" والجدال المثار حوله، لا سيما تداخله مع مفاهيم أخرى، مثل " الحروب السيبرانية" و"الجريمة المنظمة"، كما تقترح إطارا نموذجيا لتعزيز الأمان في الفضاء السيبراني وهو يشمل النواحي الإستراتيجية والتشريعية والتقنية بما يعزز الحفاظ على السلم والأمن العالميين.

الكلمات المفتاحية: الفضاء السيبراني، الإرهاب السيبراني ، تحديات الامن السيبراني ، مخاطر الارهاب السيبراني.

Abstract:

The development of information and communications has brought about a comprehensive revolution in all aspects of life, which marked the emergence of a new environment for interaction between individuals, societies and countries, termed as cyberspace, this space characterized by rapid development, and extreme ambiguity, has contributed in different ways and multiple ways - including complex And the easy one - in the development of forms of crime on all social, economic, cultural and political levels....

What has enhanced the danger of this technology, is that it transcends national borders and the spread of its networks globally, as the threats of cyberspace are not limited to the national level, but today extend to threats to the security and safety of states.

One of the most important crimes that constitute the cyberspace as an addition and a decisive turning point for it is cyber terrorism, as it is one of the crimes whose effects are reflected at the national and international levels.

Therefore, this research paper discusses the specificity and nature of the concept of "cyber terrorism" and the controversy surrounding it, especially with its overlap with other concepts, such as "cyber wars" and "organized crime". In order to enhance the maintenance of world peace and security.

Keywords: cyberspace, cyber terrorism, cyber security challenges, cyber terrorism risks.

المقدمة

يعتبر الإرهاب من الجرائم القديمة التي عانت منها جل الدول ولاتزال، حيث أنه يشكل تهديدا خطيرا على الأمن الوطني والدولي على حد سواء، ويخلف آثارا كبيرة على أمن المواطنين واستقرارهم، إذ ازدادت خطورته مع مرور الزمن وتَطوُر العلم وتوالي الاختراعات التي ابتكرها العقل البشري، فبينما كان الإرهابيون يعتمدون سابقا على وسائل تقليدية من قنابل ومتفجرات وأسلحة لتحقيق أهدافهم، أصبحوا اليوم يعتمدون على تقنيات حديثة أهمها شبكة الإنترنت، بحيث أصبحت خير وسيلة إعلامية لنشر أفكارهم وتسهيل الاتصال بينهم أو تنسيق عملياتهم، أو حتى بتوظيفها في تنفيذ أنشطة إرهابية، وابتكار أساليب وطرق إجرامية متقدمة.

ونظرا لما توفره هذه التقنيات الحديثة من خدمات، عجلت ببروز نوع جديد من الإرهاب: وهو الإرهاب السيبراني، والذي يعتبر من أخطر أنواع الجرائم التي ترتكب عبر شبكة المعلومات الدولية، بمختلف أشكاله وأنواعه، فضلاً عن تنوع الأساليب المستخدمة من لدن مرتكبيه؛ مشكلا بذلك بيئة استراتيجية ملائمة لاستقطاب أشكال جديدة من الجرائم الرقمية وانتشاره على المستويين الداخلي والدولي؛ وهوما حتم على الأجهزة الأمنية تنسيقاً إلكترونياً عالي المستوى لإيجاد سبل لمكافحته والحدّ من خطورته.

ويعتبر الإرهاب السيبراني النسخة الالكترونية عن الإرهاب التقليدي، فمن حيث التنظيم فهو عابر للحدود الإقليمية، متعدد الجنسيات لا تجمعه قضية وطنية أو قومية، بل إيديولوجية سياسية أو دينية، ويهدف إلى تحقيق أكبر الخسائر المادية والبشرية، في ظرف وجيز جدا وبسرعة البرق مستعملا في ذلك أسلحة رقمية جد متطورة[76].

وتكمن أهمية دراسة هذا الموضوع في إلقاء الضوء على جريمة الإرهاب السيبراني من خلال تحديد مفهومه، خصائصه، حجم المخاطر التي يخلفها وانعكاساته على المجتمعات، وتبيان الآليات الكفيلة لمكافحته والوقاية منه على الصعيد الدولي أو الإقليمي.

وإذا كانت الشبكة الدولية للمعلومات تشكل بيئة خصبة لاستقطاب كل أشكال التفاعلات على الصعيد المعلوماتي، فهي بالمقابل بيئة مناسبة أيضاً لممارسة ونشر العمليات الإرهابية على اختلاف صورها. ومن هنا تحدّدت مشكلة الدراسة في الكشف عن ماهية هذا الوجه الجديد للإرهاب "السيبراني" المعتمد على الهجمات

[76] 3-إيمان بن سالم، جريمة التجنيد الالكتروني للإرهاب وفقا لقانون العقوبات الجزائري، ط1 ، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، ألمانيا، 2018 ، ص 01

والجرائم الالكترونية، وما هو الخطر الذي يشكله، وما هو التوظيف الإرهابي للفضاء الالكتروني، ليصبح أزمة وتهديدا عالميا جديدا؟ وما هي أهم الاستراتيجيات الوطنية والدولية لمواجهته؟

وللإجابة على هذه الإشكالية، سوف نتطرق إلى ماهية جريمة الإرهاب السيبراني (**المطلب الأول**) ثم لمخاطر وآليات مواجهته (**المطلب الثاني**).

المطلب الاول: ماهية الارهاب السيبراني

على الرغم من أنّ جوهر الإرهاب يظل واحدا من حيث استخدام العنف أو التهديد باستخدامه من أجل إثارة الخوف والهلع في المجتمع، فإنّ أشكال الإرهاب وأدواته وأساليبه تختلف وتتطور مع مرور الزمن، فقد أدى اتساع نطاق ثورة الاتصالات والتطور التكنولوجي المذهل الذي ألغى الحدود والفواصل الجغرافية بين الدول وبسبب طبيعة شبكة معلومات الإنترنت وانفتاحها غير المحكوم أخلاقياً وسياسياً وثقافياً وقانونياً وتجارياً وصعوبة الرقابة والمساءلة على ما ينشر فيها، تبدل نمط الحياة وتغيرت معه أشكال الأشياء وأنماطها ومنها ولا شك أنماط الجريمة والتي قد يحتفظ بعضها باسمها التقليدي مع تغيير جوهري أو بسيط في طرق ارتكابها، ومن هذه الجرائم الحديثة في طرقها والقديمة في اسمها جريمة الإرهاب السيبراني والتي أخذت أشكال حديثة تتماشى مع التطور التقني، لهذا كان لزاما علينا التطرق لمفهوم الارهاب السيبراني (**الفقرة الأولى**)، ثم لخصائصه ودوافعه (**الفقرة الثانية**).

الفقرة الاولى: مفهوم الإرهاب االسيبراني

تنوعت تعاريف "الارهاب السيبراني" إذ ليس هناك تعريف متفق عليه دوليا، بسبب تنوع وجهات النظر (**أولا**)، ثم تعدد أساليب وأشكال وأنواع هذا الإرهاب المستحدث (**ثانيا**).

أولا : تعريف الإرهاب[77] االسيبراني

---

[77] كلمة الإرهاب كلمة دخيلة على مصطلحات اللغة العربية "فقد أقر المجمع اللغوي كلمة الإرهاب ككلمة حديثة في اللغة العربية وأصلها "رهب " بمعنى خاف وإرهاب مصدر الفعل "أرهب" ويعني أخاف وأفزع ورهبه اي أخافه وراهب من الله تذل على خشيته والخوف من عقابه

- توفيق شريخي، الإرهاب الالكتروني وتأثيره على أمن الدولة مذكرة مقدمة لنيل شهادة الماستر ، سنة 2017ـ2018 ص 9.

- وقد أطلق مجمع اللغة العربية في معجمه الوسيط على الإرهابيين أنه وصف يطلق على الذين يسلكون سبيل العنف لتحقيق أهدافهم ، فكلمة إرهاب تستخدم للخوف والرعب الذي يسببه فرد أو جماعة سواء كان لأغراض سياسية أو شخصية.

=

يتألف مصطلح الإرهاب السيبراني (cyberterrorisem) من كلمتين كلمة(cyber) تعني الانترنت و (terrorisme) تعني الإرهاب ، ولقد ظهر هذا المصطلح عقب التطورات الكبيرة التي حققتها تكنولوجيا المعلومات واستخدام الحواسب الآلية والانترنت في إدارة معظم شؤون الحياة .

حيث نجد أن الغرب أول من تفطن لهذا الإرهاب السيبراني أو ما يسمى الرقمي أو المعلوماتي أو الشبكي حيث تعددت تسمياته، في فترة الثمانينات وأقر "Barry Collin " فأول من استخدام كلمة الارهاب السيبراني وعرفه أنه" هجمة الكترونية غرضها تهديد الحكومات أو العدوان عليها سعيا لتحقيق أهداف سياسية أو دينية أو ايدلوجية وان الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب" [78].

ولقد ظهر الإرهاب السيبراني بشكل علني في الولايات المتحدة الأمريكية عندما قام الرئيس بيل كلينتون سنة 1996 بتشكيل لجنة حماية منشآت البنية التحتية، التي توصلت إلى أن مصادر الطاقة والاتصالات

ولا يختلف معنى الإرهاب كثيرا في اللغة الإنجليزية عن نظيره في اللغة العربية تعني (terrorisme) يعني الشعور بفزع أو الخوف الشديد وكلمة (terrorize) فافعل استعمال العنف من اجل تحقيق أهداف سياسية أو إرغام الحكومة بقيام بعمل ما .وهي ترادفها كلمة رعب (terreur) حيث نجد في اللغة العربية كلمة (terror) مشتقة من كلمة ذعر أو رهبة كما ترادفها اصطلاحا كلمة إرهاب محمد حسن عمر برواري، غسيل الأموال وعلاقته بالمصارف والبنوك، دراسة مقارنة، دار قنديل لنشر والتوزيع، عمان، ط1 ، 2013 ص 182.

أما في اللغة الفرنسية "وردت كلمة إرهاب في قاموس لاروس بمعنى مجموعة من أعمال العنف من أجل تحقيق أهداف سياسية أما في اللغة الإنجليزية فوردت كلمة إرهاب في قاموس أكسفورد بأنه استخدام للعنف والتخويف بصفة خاصة ضد حكومات الدول أو الشخصيات المهمة أو الأشخاص الآخرين التابعين للدولة- محمد أقبلي وعابد العمراني : القانون الجنائي المعمق في شروح - الطبعة الأولى 2020 ،ص 93.

- كما عرفه أيضا احمد جلال عز الدين بأنه" عنف منظم ومتصل بقصد خلق حالة من التهديد العام الموجه إلى دولة أو جماعة سياسية والذي ترتكبه المنظمة بقصد تحقيق أهداف سياسية عبد القادر زهير النقوزي، مفهوم القانوني لجرائم الإرهاب الداخلي والدولي، منشورات حلبي الحقوقية، ط1 ، بيروت، 2008 ، ص2

بينما عرفه الدكتور محمد إبراهيم زياد على انه " اللجوء إلى العنف أو تهديد بالعنف من جانب جماعة ترمي إلى تحقيق هدف يتعارض مع أهداف السلطة التشريعية" محمد إبراهيم زيد، مقدمة في علم الاجرام وعلم العقاب، دار الهدى للمطبوعات، الإسكندرية، 2008 ، ص2

كما أنه جاء في الموسوعة السياسية أن الإرهاب هو استخدام العنف الغير القانوني أو التهديد به بغية تحقيق هدف سياسي ليندا بن طالب، غسيل الأموال وعلاقتها بمكافحة الارهاب، دراسة مقارنة، دار الجامعة الجديدة لنشر، الإسكندرية، 2011، ص1

وعرفه ليمكن lemkin بأنه تخويف الناس بمساهمة أعمال العنف دون النظر للغرض والهدف من ذلك.

أما سوتيل SOTTIL فيعرف الإرهاب أنه عمل إجرامي مصحوب بالرعب أو العنف بقصد تحقيق هدف محدد.

أما ولتر WELTER فقد عرف الإرهاب بأنه عملية رعب تتألف من ثلاث عناصر العنف والتهديد باستخدامه والخوف الناتج عن ذلك للمزيد من التفصيل يرجى الاطلاع على - محمد أقبلي وعابد العمراني م .س : ص 94

[78] عادل عبد الصادق، استخدام الإرهاب الالكتروني في الصراع الدولي، دار الكتاب الحديث، القاهرة،2015 ص104

وكذا شبكات الكمبيوتر ستكون الهدف الأول للهجمات الإرهابية، ولكن هذه الأخيرة لم تعرفه واكتفت بدراسة الظاهرة ومحاولة فهم سياسة تفكير الإرهاب الالكتروني والطرق التي يتخذها في تنفيذ عملياته بحيث تظهر الدراسة شغف الإرهابيين في استخدام شبكة الانترنت في عملياتهم الإرهابية، مظهرين بذلك براعتهم في التفوق على أية تقنية مستخدمة [79].

وفي هذا الصدد قامت وكالة المخابرات المركزية الأمريكية بتعريف الإرهاب السيبراني على أنه" أي هجوم تحضيري ذو دوافع سياسية موجهة ضد نظم المعلومات والتي تنتج عن العنف ضد الأهداف المدنية عن طريق جماعات دون قومية أو عملاء سريين[80] "

في حين عرفه مركز حماية البنية التحتية القومية الأمريكية" أنه عمل إجرامي يتم تحضيره عن طريق استخدام أجهزة الكمبيوتر والاتصالات السلكية ولا السلكية ينتج عنه تدمير وتعطيل الخدمات لبث الخوف بهدف إرباك وزرع الشك لدى السكان وذلك بهدف التأثير على الحكومة أو السكان لخدمة أجندة سياسية أو اجتماعية أو ايدلوجية[81] "

ويرى مجمع الفقه الإسلامي أن الإرهاب السيبراني هو " العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية ويكون صادرا عن الدول أو الجماعات أو الأفراد على الإنسان أو دينه أو نفسه أو عرضه أو عقله أو ماله ، بغير حق بشتى صنوفه (العدوان) وصور الإفساد في الأرض ".

أما على مستوى الاتفاقيات الدولية فقد عرفته الاتفاقية الأولى لمكافحة الإجرام عبر الإنترنيت في بودابست عام 2001 " بأنه هجمات غير مشروعة أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونيا توجه من أجل الانتقام أو الابتزاز أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة "

---

[79] نجاري بن حاج علي فايزة، الاليات القانونية للإرهاب الالكتروني، مذكرة ماجستير في القانون الدولي لإعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2016 ، ص24

[80] -عادل عبد الصادق، المرجع السابق، ص106

[81] توفيق مجاهد، طاهر عابسة، جريمة الإرهاب في ضوء احكام الاتفاقية العربية لمكافحة ج ا رئم التقنية المعلومات، لعام 2010 ، مجلة العلوم القانونية والسياسية، المجلد 09 ، العدد 03 ، ديسمبر 2018 ، ج ا زئر، ص82

كما عرفه بعض الفقه[82] بأنه" يعني العدوان أو التخويف أو تهديد ماديا أو معنويا باستخدام الوسائل الالكترونية الصادرة من دول أو جماعات أو الأفراد عبر الفضاء الالكتروني أو أن يكون هدفا لذلك العدوان بما يؤثر على الاستخدام السلمي له".

وهناك من عرفه[83] بأنه " هجمات غير مشروعة أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة الكترونيا توجه من اجل الانتقام والابتزاز أو الإجبار أو التأثير على الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة وبتالي لكي يلقب الشخص ما بأنه إرهابي على الانترنت وليس مخترقا فقط فلا بد من أن تؤدي الهجمات التي يشنها إلي عنف ضد الأشخاص أو على الأقل تحدث أذى كافيا من اجل نشر الخوف والرعب". ولقد عرفه أخر[84] بأنه "خرق للقانون يقدم عليه فرد من الأفراد أو تنظيم جماعي بهدف إثارة اضطراب خطير في نظام العام عن طريق شبكة المعلومات العلمية الانترنت".

وتأسيسا على ما سبق يمكننا القول بأن الإرهاب السيبراني هو إرهاب حديث أفرز لنا حربا من نوع جديد تعرف بالحرب السيبرانية، التي لا تتطلب سوى معرفة اختراق الحواجز الإلكترونية ومن خلالها انتقلت المواجهة مع المنظمات الإرهابية من الصورة التقليدية إلى مواجهة إلكترونية غير مباشرة باستخدام وسائل رقمية.

ثانيا: التوظيفات الإلكترونية للمنظمات الإرهابية

تغيرت وسائل الارهاب السيبراني بتغير صورته من التقليدية إلى الحديثة، فبعيدا عن وسائل الإرهاب التقليدي من قنابل ومتفجرات وأسلحة ...، أصبحنا أمام صورة جديدة لإرهاب سيبراني الذي يتم عبر الوسائل التكنولوجية، إذ تعمد الجماعات والتنظيمات الإرهابية إلى استخدام وسائل حديثة وغير مكلفة لتنفيذ مخططاتهم وتكمن أهم وسائل الإرهاب السيبراني في :

مواقع التواصل الاجتماعي: أصبحت مواقع التواصل الاجتماعي من فيسبوك Facebook وتويتر twitter والبريد الإلكتروني ...، من أهم وسائل الإرهاب السيبراني، حيث أنها تمكن الأفراد من التواصل والتعرف على البعض ومشاركة الآراء والاهتمامات ، كما تستخدم لتفاعل والتنسيق أثناء العمليات الإرهابية.

---

[82] عادل عبد الصادق، الإرهاب الالكتروني قوة في العلاقات الدولية نمط جديد وتحديات جديدة، ط1 ، مركز الأهرام للدراسات السياسية والاستراتيجية 2009 , ، ص109

[83] علي عدنان الفيل، الاج ا رم الالكتروني، مكتبة زين الحقوقية والأدبية، لبنان، ط1 ، 2011 ، ص60

[84] -اسراء طارق جواد، كاظم الجابري، جريمة الإرهاب الالكتروني، دراسة مقارنة، رسالة ماجستير في القانون العام، كلية الحقوق ن جامعة البحرين، العراق، 2012 ، ص23

التجسس الإلكتروني: يقوم الإرهابيون بالتجسس على الأشخاص والدول والمنظمات والهيئات والمؤسسات الدولية والوطنية الكترونيا ويتم التجسس على المجالات العسكرية والاقتصادية والسياسية ، ففي عصر المعلومات أصبحت حدود الدول مفتوحة للدول من خلال أقمار التجسس الإلكتروني في الحصول على أسرار ومعلومات الدول والمنظمات الأخرى ومن تم إفشاءها وتتم عملية إرسال نظم التجسس الإلكتروني عن طريق البريد الإلكتروني .

الهاتف الخلوي: أصبح الهاتف أحد الوسائل الالكترونية الأكثر استخداما وذك من خلال الميزات العديدة التي أصبح يتوفر عليها مما أسهم في استخدامه لأغراض إرهابية فمن خلاله يمكن أن تتم عملية تفجير السيارات والمباني والعبوات الناسفة والتي تتم برمجتها مع أجهزة الهاتف النقال .

أنظمة الهاكرز أو الاختراق :يقوم الإرهابيون المبرمجون الذين يسمون ب(الهاكرز أو قراصنة الحاسوب)باختراق المواقع أو الحواسب الإلكترونية، باستخدام برامج للتجسس على الشبكات والأنظمة الإلكترونية والاعتداء على البنية التحتية المعلوماتية للمؤسسات الحكومية والخاصة على حد سواء، ومن أشهر برامج الهاكرز (web cracker4) و (buster net) و (net bus haxporf) [85] .

ويعدّ علم الاختراق من الطرق الحديثة في التجسس الإلكتروني، إذ يعمل المتجسس الإرهابي على تسريب المعلومات الرقمية الحساسة ونقلها عن طريق إخفائها- في بداية الأمر -في وسيط إلكتروني دون إحداث أي تغيير أو تشويه بالرسالة المرسلة، بحيث لا يمكن اكتشافها والتفطن لها حتى لو تم ضبط الشخص متلبساً بالجريمة، وتعدّ من أخطر طرق التجسس ولاسيما عند استخدامها من قبل الإرهابيين[86]

الفيروسات لتدمير أنظمة المعلومات : تقوم التنظيمات الارهابية بمحاولة تخريب نقطة لاتصال او النظام عبر شبكة الانترنيت الخاصة بالأفراد والمؤسسات العسكرية والمدنية الشركات الخاصة ، عن طريق صنع أنواع من الفيروسات الجديدة التي تسبب ضرارا كبيرا لأجهزة الحاسوب والمعلومات التي تم تخزينها على هذه الاجهزة وتعد الفيروسات والديدان من أخطر الاسلحة التي تستخدمها المجاميع الإرهابية في شن هجوماتها الالكترونية ويزداد الخطر إذا دخلت على خط المواجهة والإرهاب السيبراني دول بإمكانيات واسعة المثال على

---

[85] **مايا حسن ملا خاطر، الإطار القانوني لجريمة الإرهاب الإلكتروني، مجلة جامعة الناصر، اليمن، العدد 5، سنة 2015، ص، 135.**

[86] **عبادة الحارث خليل قمر، فن الاختزال بين الحقيقة والخيال، جامعة الحسين بن طلال، الأردن، 2015 ، ص.5 :**

ذلك الفيروسات (ستا كسنت) التي طورتها الولايات المتحدة الامريكية واسرائيل للنيل من البرنامج النووي الايراني وتعطيله.

المنتديات وغرف الدردشة :عبارة عن مساحات معروفة في الفضاء الالكتروني تسمح للأعضاء المشتركين فيها بالتحدث مع بعضهم البعض، تعد من أهم وسائل الاستقطاب لدى الجماعات الإرهابية عن طريق تخصيص مستخدمي الانترنيت الذين يتقنون اللغة الاجنبية للإجابة على اسئلة الشباب الذين يسعون للتعرف على خبايا التنظيم[87].

القنابل المعلوماتية :يمكن تقسيمها على نوعين :**القنابل المنطقية** التي تعرف بأنها البرمجية التي يتم تداولها بكثرة في البرمجيات سواء المقتناة أو عبر الإنترنت، وهي عبارة عن جزء سري من البرمجية ينفجر فيبطل عملها، **والقنابل الزمنية** وهي برمجية توضع في النظام المعلوماتي لتنفجر في تأريخ معيّ يحدده صانعها لتسبب أضراراً للنظام المعلوماتي[88].

الفقرة الثانية : خصائص الإرهاب السيبراني ودوافعه

تتصف جريمة الارهاب السيبراني بخصائص تميزها عن غيرها من الجرائم الالكترونية، (**أولا**) وكذلك تنوع دوافعه (**ثانيا**).

أولا: خصائص الارهاب السيبراني

صعوبة الاثبات : إن الجرائم الإلكترونية صعبة من حيث إثباتها نظرا لسرعة غياب الدليل الرقمي وسهولة إتلافه وتدميره .

صعوبة اكتشاف جرائم الإرهاب السيبراني: إن مرتكبوا هذه الجرائم لهم صفات مميزة من حيث الثقافة والعلم التكنولوجي والخبرة في الميدان مما يصعب على بعض الاجهزة الأمنية والقضائية اكتشاف الجرائم الإلكترونية لوجود نقص كبير في الخبرات في مثل هذه الجرائم المستحدثة دائمة التطور والتغير.

لا حدود جغرافية لها: الغت شبكة الانترنيت اي حدود جغرافية فيها بين الدول فهو لا يخضع لأي نطاق جغرافي معين لأنه يتم في بيئة إلكترونية.

---

[87] ـ بن صفية وداد، مذكرة مقدمة لنيل شهادة الماستر الأكاديمي تأثير المتغير التكنولوجي على الفواعل الدولية الجديدة للإرهاب الإلكتروني ـ أنموذجا ـ 2018 ـ 2017 ص 54

[88] زين العابدين عواد كاظم الكردي، جرائم الإرهاب الإلكتروني(دراسة مقارنة)، منشورات الحلبي الحقوقية، بيروت، ط1 ، 2018، ص 120.

البيئة الهادئة: إن تحقق الإرهاب الإلكتروني يقتضي فقط وجود حاسب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج فالإرهاب الإلكتروني يحدث في بيئة هادئة لا تحتاج الى القوة والعنف واستعمال الأسلحة ولذلك يطلق عليه الجرائم الناعمة ، كل ما يحتاجه هو جهاز حاسب آلي وشبكة انترنيت ، فنقل البيانات من الحاسب الآلي او السطو الإلكتروني لا تحتاج إلى عنف أو إطلاق نار .

جريمة حديثة : ظهرت الجرائم الإلكترونية مع تطور وسائل التكنولوجيا حيث أنه قديما لم يعرف هذا النوع من الإرهاب ولا يمكننا الإنكار بأن العامل البشري هو المحرك الاساسي لتفشي هذه الظاهرة ، إذ يتصف مرتكبيها بالذكاء والمهارة و الاحتراف، في مجال الحاسب الآلي وشبكة المعلوماتية .

ثانيا: دوافع الإرهاب السيبراني

مع تطور وسائل التكنولوجيا، أقبل عليها المجتمع بشكل غير عادي نظرا لما تقدمه من خدمات كبيرة إلا أنه سعى الإرهابيون إلى الاستفادة منها لصالح الشر ونشر أفكار الكراهية والعدوان في عقول المستخدمين مما نتج عنه عدة جرائم من أبرزها جريمة الإرهاب الإلكتروني التي تعتبر من أخطر أنواع الجرائم التي ترتكب عبر شبكة المعلومات الدولية . بحيث تعددت دوافعه واختلفت في درجة الأهمية تبعا للظروف التي تساعد على تحققه، إذ تنقسم إلى دوافع عامة وأخرى خاصة.

1 : الدوافع العامة

أ: الدوافع السياسية

يعتبر العامل السياسي من أهم الأسباب التي تدفع للإرهاب السيبراني، ففي ظل غياب الديمقراطية والحرية وتهميش المواطنين ومعاناتهم من الظلم والاضطهاد والسيطرة الاستعمارية إضافة إلى سلب حقوقهم وحرمانهم من حرية الرأي والتعبير وعدم المساواة في توزيع الثروة الوطنية والتفاوت في توزيع الخدمات والمرافق العامة والتقصير في أمور الرعية كل هذا أدى إلى ظهور منظمات سرية وردود أفعال غاضبة انصبت في شكل الإرهاب.

ب: الدوافع الاجتماعية

يعد السلوك الإجرامي سلوك مكتسب نتيجة لتفاعل عدة عوامل إذ أن التفكك الأسري والاجتماعي والجهل والفراغ النفسي والعقلي، أدى إلى أمراض نفسية وتقبل كل أفكار التطرف.

ج: الدوافع الاقتصادية

يلعب الدافع الاقتصادي دورا مهما في تفشي ظاهرة الإرهاب نظرا للتفاوت الطبقي والاجتماعي وعدم المساواة ومعاناة الأفراد من الفقر والبطالة وأزمات السكن و التضخم في أسعار المواد الغذائية والخدمات الأساسية كما أن التقدم في الأنظمة المصرفية الذي سهل تحويل الأموال حول العالم عن طريق الأنترنيت ساعد المنظمات الإرهابية على استغلال الفرصة من أجل تحقيق أهدافها الغير المشروعة .

د: دوافع إيديولوجية :التعصب لمبدأ فكرى أو دينى قد يدفع الى اللجوء الى استعمال العنف وممارسة الارهاب من قبل فئة معينة تحاول فرض مبادئها على المجتمع.

2 : الدوافع الخاصة

من الدوافع الخاصة التي تؤدي إلى انتشار ظاهرة الإرهاب السيبراني ، نجد انخفاض التكلفة، وسهولة الاستخدام حيث أن الوسائل الالكترونية تعرف انخفاضا في الثمن مقارنة مع الوسائل التقليدية التي تتم بها العمليات الارهابية فهي لا تستغرق وقتا طويلا ولا مجهودا كبيرا مما مكن الارهابيين من تحقيق هدفهم والوصول الى مبتغاهم كما ، أن غياب الرقابة على الأطفال والشباب في المنزل والمدرسة نتج عنه الاستخدام غير المعقلن لوسائل التكنولوجيا، إضافة إلى الفراغ الذي يعاني منه الكثير من الشباب الذي يدفعهم إلى استخدام التكنولوجيا والوقوع في يدي الإرهابيين عن طريق مواقع التواصل الاجتماعي.

وفي نفس الاطار نشير إلى أن إلغاء الحدود الجغرافية وتدني مستوى المخاطرة يعد فرصة بواسطتها يستطيع محترف الحاسوب أن يتخفى تحتها بشخصية وهمية ويقدم نفسه بالهوية والصفة ويطلق على نفسه ألقاب وأسماء مستعارة ويؤديها بأدلة مادية ملموسة أو بعض المعلومات الصحيحة ليثبت مدى جديته ومن تمة يستطيع أن يشن هجومه الإلكتروني دون تعريض نفسه لمخاطرة مباشرة .

كما أن غياب الرقابة على الشبكات المعلوماتية يعد من الأسباب الرئيسية في انتشار الإرهاب السيبراني ففي الكثير من الأحيان يصعب على اجهزة الشرطة ملاحقة القائمين بعملية الإرهاب السيبراني والتعرف على هويتهم [89] .

[89] ـ جبار حسن ـ زينب كاطع ناهض، المرجع السابق، ص : 9

المطلب الثاني : مخاطر جريمة الارهاب السيبراني وآليات مواجهته.

في ظل انتشار جريمة الإرهاب السيبراني وما تشكله هذه الجريمة من مخاطر على كل القطاعات الحيوية في الدول وعلى كل الجوانب سواء الاقتصادية أو السياسية أو السياسية أو الأمنية (**الفقرة الأولى**)، سعت الدول جاهدة من أجل التصدي لها، وذلك بوضع مختلف الإجراءات للحد من انتشار هذه الجريمة (**الفقرة الثانية**).

الفقرة الأولى : مخاطر الإرهاب السيبراني .

تكمن خطورة الارهاب السيبراني في سهولة استعمال وسائل التكنولوجيا المتطورة، فهو يشكل خطر على التجارة الالكترونية (**أولا**)، إضافة إلى شدة أثره وضرره على كل مجال الحياة والقطاعات الحيوية للدول (**ثانيا**).

أولا المخاطر الأمنية للإرهاب السيبراني على التجارة الالكترونية

تتفاقم يوما بعد يوم مخاطر الإرهاب السيبراني نظرا لاستعماله لتكنولوجيات الحالية بإضافة إلى الثغرات الأمنية المتعددة في التعاملات التجارية الالكترونية وتتجلى أهم هذه المخاطر في:

1: القرصنة أو تعطيل نظام المعلومات:

والقرصنة السيبرانية تتمثل في عملية نسخ البرمجيات غير المصرح به، أو إعادة إنتاجها، أو استخدامها أو تصنيع نسخ بطريقة غير شرعية أو نشر وتوزيع المنتج البرمجي أو استغلاله على نحو مادي أو تقليدها أو محاكاتها والانتفاع بها على نحو يخل بحقوق الدول والمؤسسات بدون الحصول على إذن أو تفويض[90].

و تعتبر الفيروسات وسيلة هجوم شائعة لإتلاف معطيات التعاملات التجارية من قبل الإرهابيين ولكن هناك عدة مخاطر للقرصنة أو تعطيل نظام المعلومات تتبين فيما يلي:

أ: **خرق الحماية المادية:** ويتم ذلك عن طريق

- **التفتيش في المخلفات التقنية** : ويقصد بها بحث الإرهابيين في مخلفات المؤسسة عن شيء يساعدهم في اختراق نظام المعلوماتي للمؤسسات التجارية والمالية مثل أوراق مكتوب عليها كلمة السر أو مخرجات الكمبيوتر أو الأقراص الصلبة المرمية بعد استعمالها أو ما شابه ذلك.

---

[90] خالد مصطفى فهمي، الحماية القانونية لبرامج الحاسب الآلي في ضوء - قانون حماية الملكية الفكرية طبقا لأحدث التعديلات- ، دراسة مقارنة، بدون ناشر، 2005، ص 210.

- **الالتقاط السلكي** :هو توصيل السلك المادي مع شبكة توصيلات النظام لجهة استراق السمع بطريقة سهلة أو معقدة تبعا لنوع الشبكة أو طرق التواصل المادي[91].

ب: **خرق الحماية المتعلقة بأشخاص وشؤون الموظفون :**

- **التخفي بانتحال شخصية موظف** :وهو استخدام الإرهابي لوسائل التعريف العائدة للموظف المخول له هذا الاستخدام كاستغلال أحد الإرهابيين لكلمة سر أحد العمال، واستغلال صلاحيات مخولة للموظف من خلال اقتناص شخصيته[92] .

2: جرائم التجسس الاقتصادية والتجارية

وهي جرائم التجسس التي يكون الهدف منها الحصول على معلومات اقتصادية وتجارية. ويعد التجسس الصناعي نوعا من التجسس ينفذ لأغراض تجارية وتقوم به بعض الشركات والمؤسسات التجارية بهدف الحصول على أسرار صناعية من الشركات المنافسة، وهذا النوع من التجسس غالباً ما يرتبط بالصناعات التقنية، مثل البرمجيات والتقنية الحيوية، وتقنيات الفضاء والاتصالات والمواد والطاقة.

وتسعى الجماعات الإرهابية من خلال التجسس على المعلومات الصناعية والمالية والتجارية إلى ضرب مواقع القوى الاقتصادية لدولة ما والضغط عليها من خلال ابتزازها بطلب فدية أو إطلاق سراح الرهائن[93].

كما تعتبر الشبكة العنكبوتية سوق مفتوح لجميع الدول تتم من خلالها التعاملات بمبالغ ضخمة تصل إلى مليارات الدولات مما يجعل الجانب الاقتصادي للأنترنت الأكثر خطورة، لأن الهدف الأساسي للإرهاب هو المال والثاني أن الهجمات الموجودة ضد نظم المعلومات الاقتصادية لها تأثير كبير على الرأي العام[94].

3: اختراق الإرهاب السيبراني لموقع التجارة الالكترونية

إن التهديدات التي تواجه التجارة الالكترونية في تزايد مستمر كلما تطورت التكنولوجيا نذكر منها:

---

[91] نجاري بن حاج علي فايزة، الآليات القانونية للإرهاب الالكتروني، مذكرة ماجستير في القانون الدولي لإعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2016، ص 43.

[92] سعاد إكرام عوض، التزوير المعلوماتي، دراسة نقدية لمختلف القوانين الوضعية، منشأة المعارف، الإسكندرية،2008، ص1

[93] حكيم غريب، مكافحة الاشكال الجديدة للإرهاب الدولي، رسالة دكتورة، كلية العلوم السياسية و العلاقات الدولية، جامعة الج ا زئر 03 ، الجزائر ، 2014 ، ص 840.

[94] -سهيلة خليل غازي، معوقات التجارة الرقمية في الدول العربية، دار الوفاء لنشر، القاهرة، مصر، 2003 ، ص 106

أ: انتهاك نظام الحماية السرية للتجارة الالكترونية

يقوم الإرهاب السيبراني بالوصول إلى المعلومات المالية والشخصية واختراق الخصوصية وسرية المعلومات بسهولة، ذلك راجع للتطور الهائل لجهاز الحاسوب، وخصوصية مرتكبو الجريمة المعلوماتية فهي ترتكب بواسطة خبراء جهاز الحاسوب وليس أشخاص عاديين[95].

ب: إتلاف مواقع التجارة الالكترونية باستخدام الفيروسات

بما أن التجارة الالكترونية تعتمد في تصرفاتها على نظام الحاسب الآلي المتصل بالشبكات المعلومات كأحد الآليات التي يتم من خلالها ممارسة مختلف النشاطات التجارية والالكترونية، فإن الفيروس المعلوماتي الذي ينشط هو الأخر على نفس مستوى التجارة الالكترونية، يتميز بخاصيتين في غاية الخطورة أولها الانتقال والانتشار والثانية التدمير.

أما بخصوص انتقال وانتشار الفيروس، فهو ينتقل من جهاز إلى آخر بسرعة يساعده في ذلك وجود وسائل اتصال حديثة، أما بخصوص اثر الفيروس في التدمير فانه يرتبط ببرنامج معين يدخل إليه المستخدم وبعد تاريخ و ساعة معينة يبدأ الفيروس في التدمير الذي يشمل مسح البيانات المخزنة، ومن أعراض الإصابة بالفيروس بطئ نظام التشغيل، ضيق سعة التخزينية كما يؤدي إلي تشويش المعلومات وكذا ادخال معلومات غير صحيحة[96].

ثانيا: آثار الإرهاب السيبراني

خلفت العمليات الإلكترونية العديد من الآثار تؤثر على أمن واستقرار الدولة والمواطنين وعلى الإمكانيات الاقتصادية والهيبة السياسية للدولة بحيث أن الإرهاب السيبراني ذو طابع دولي، وهو بذلك يشكل تهديدا على أمن الدولة ومنشآتها المختلفة وعليه فهو امتداد للجريمة العابرة للقارات حيث اتخذت الجرائم الإرهابية عبر الوسائل الإلكترونية أشكالا أنتجت آثارا ضارة على العلاقات الدولية وأصبحت تهدد الأمن والسلم الدوليين.

كما تظهر خطورة الإرهاب السيبراني في المجالات الاقتصادية السياسية والثقافية والاجتماعية والنفسية والأمنية فمن الناحية الاقتصادية فإن العمليات الارهابية تؤثر على التنمية الاقتصادية للدولة نتيجة لما تخلفه من خسائر مما يؤدي إلى انخفاض حجم التبادلات الخارجية.

[95] **علاء الصراط الغامدي، الحرب النفسية للإرهاب الجديد، دار منشاة المعارف، الإسكندرية، مصر، 2006 ، ص 50.**

[96] **نجاري بن حاج علي فايزة، المرجع السابق، ص 54.**

- انعدام الأمن الاقتصادي الذي يؤدي الى تغيير العادات الاستهلاكية والادخار الاستثمار.
- إنخفاض تدفق رؤوس الأموال والاستثمار المباشر الأجنبي
- تعطيل المصارف والمعاملات المالية الدولية والبورصات لإفقاد الثقة في النظام
- تغير مكونات صناعة الأدوية عن بعد لدى شركات الأدوية
- تغيير الضغط في خطوط الغاز مما يوقع انفجارات وحرائق مروعة.
- مهاجمة أنظمة التحكم في الحركة الجوية وجعل الطائرتين مدنيتين تتصادمان عن طريق الولوج إلي أجهزة استشعار في قمرة القيادة الطائرة وهذا ممكن في خطوط السكك الحديدية أيضا.

وأما من الناحية النفسية فإن عدم الشعور بالأمن والطمأنينة وفقدان الثقة يؤدي إلى انتشار الأمراض النفسية ويمكن تحديد أهم الآثار النفسية التي يتركبها الإرهاب السيبراني زيادة الأمراض النفسية على الفرد نتيجة عيشه حالة قلق توتر واضطراب مستمر وصراع نفسي دائم بسبب الوضع الناجم عن هذه الأعمال الارهابية والاعتداءات الوحشية العشوائية على الوسائل الإلكترونية

- تأثر الأطفال نفسيا بما يشهدونه من أحداث ارهابية عبر الوسائل الالكترونية خاصة الآثار الدموية التي يخلفها الإرهاب وبشكل خاص إذا كان الضحايا من أسرة الطفل.
- التهديد بعدم الاستقرار لدى الأشخاص نتيجة الاكتئاب والقلق مما ينعكس على سلوكياتهم وتعاملهم مع الآخرين، الأمر الذي يؤدي إلى ضعف العلاقات بين أفراد المجتمع القائمة على أساس الثقة والاطمئنان الغير[97].

أما من الناحية الثقافية فإن الإرهاب الإلكتروني يقلل من الدوائر الثقافية والعلمية فقد اغتيل رجال ونساء كانت مهنتهم الابداع الأدبي والفني وظل البعض الآخر يشد الرحال بعيدا عن الوطن هروبا من العنف كما تهجم الإرهاب ايضا على التراث المادي والمعنوي وكذلك البنى التحتية الثقافية .

ومن آثار الإرهاب السيبراني على الناحية السياسية فإنه يهدد الوحدة الدولية بالتفكك فضلا على النيل من سمعة الدول وهيبتها أمام الرأي العام الدولي ويضعف أو ينعدم ثقلها السياسي. ومن حيث الناحية الاجتماعية أثر الإرهاب على الحقوق الاجتماعية بحيث ساهم في انتشار البطالة واستفحال ظاهرة التهرب المدرسي.

---

[97] -عبد الله عبد الكريم عبد الله، جرائم المعلوماتية الانترنت (الجرائم الالكترونية)، ط1 ، منشورات حلبي الحقوقية، بيروت، 2007، ص، 32 .

أما الآثار الأمنية التي يخلفها الإرهاب السيبراني فتتمثل في :

-انعدام الشعور بالأمن الإلكتروني وعدم الطمأنينة والخوف في مجال الحياة العادية نتيجة حالة القلق الدائم الذي يعيشه الفرد حيث لا يدري متى سيصيبه الخطر الناتج عن الارهاب السيبراني[98] .

- تعمل المنظمات الإرهابية عبر الوسائل الالكترونية الى التحكم بالأنظمة الأمنية من خلال فك الشفرات السرية للتحكم بتشغيل منصات إطلاق الصواريخ الاستراتيجية[99].

الفقرة الثانية : الإجراءات المتخذة لمكافحة الإرهاب السيبراني .

إن الإرهاب السيبراني ظاهرة عابرة للحدود تتطلب اتخاذ إجراءات لمنع إساءة استعمال الإرهابيين والمتطرفين العنيفين للتطورات التكنولوجية والتصدي لمخططاتهم وفي هذا الشأن اتخذت المؤسسات الدولية (**أولا**) والدول على عاتقها سن عدة اتفاقيات لمعالجة موضوع الارهاب السيبراني (**ثانيا**).

أولا: جهود المؤسسات الدولية في مجال مكافحة الإرهاب السيبراني

- **قرارات ووثائق الأمم المتحدة:** في نطاق العمل الأممي، أصدرت الأمم المتحدة عدة قرارات بخصوص الجرائم السيبرانية أو المعلوماتية، أهمها القرار رقم 55-63 بتاريخ 4 ديسمبر 2000 والقرار رقم 56-121 بتاريخ 19 ديسمبر 2001 حول محاربة سوء استخدام تكنولوجيا المعلومات، وقد أوصى القرار 55-63 بأن تضمن الدول في قوانينها وممارساتها إلغاء أية ملاذات آمنة لكل من يسيء استخدام تكنولوجيا المعلومات، كما أقر بأن الأنظمة القانونية يجب أن تحمي سرية المعلومات وأنظمة الحاسوب وسلامتها من أي اعتداء غير مشروع، وأن تضمن معاقبة التصرف الجرمي، ويدعو القرار 56-121 الدول عند صياغة قوانين وطنية أو سياسات أو ممارسات لمحاربة سوء الاستخدام الجزائي لتكنولوجيا المعلومات، أن تأخذ في الحسبان أعمال وإنجازات لجنة الوقاية من الجرائم والوقاية الجزائية[100].

---

[98] عمراني كمال الدين، السياسة الجنائية المنتهجة ضد الجرائم الالكترونية، دراسة مقارنة، أطروحة دكتورة، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان،2012 ، ص 100.

[99] ـ شاشوة ياسمينة المرجع السابق، ص ، 63

[100] نشير إلى هناك عدة اتفاقيات في هذا الشأن؛ منها الاتفاقية الدولية لمكافحة الإرهاب والجريمة الالكترونية التي وقعتها عام 1999 أكثر من (26) دولة وكذلك اتفاقية (بودابست 2001) للجرائم الإلكترونية التي تعكس الجهد الواسع والمميز للاتحاد الأوروبي ومجلس أوروبا .

وتبعها اتفاق الدول الصناعية الثماني الكبرى في مؤتمرها السنوي بألمانيا عام 2007 على خطة لمواجهة الإرهاب الإلكتروني على مستوى العالم إلى جانب إصدار الإعلانات الدولية وسن القوانين الوطنية.

=

وقد أصدرت الجمعية العامة للأمم المتحدة في عام 2005 القرار رقم 177-60 الذي يشجع التعاون لمكافحة الجرائم السيبرانية وتقديم المساعدة للدول الأعضاء في هذا المجال، كما أصدرت الأمم المتحدة عام 2010 القرار 211-64 الذي يدعو الدول إلى تحديث قوانينها في مجال الجرائم السيبرانية والخصوصية والبيانات الشخصية والتجارة والتواقيع الإلكترونية، وإلى اعتماد الاتفاقيات والتجارب الإقليمية في هذه المراجعة.

جهود الإتحاد الدولي للاتصالات: أعلن الأمين العام للاتحاد الدولي للاتصالات عام 2007 إطلاق مبادرة أجندة الاتحاد الشاملة حول الأمن السيبراني، ويعمل الإتحاد الدولي منذ ذلك العام على هذه الأجندة التي تهدف إلى إنشاء إطار أو بروتوكول للتنسيق بين جهود مكافحة الجرائم السيبرانية، وهو يشمل تدابير قانونية وتقنية وتدابير إجرائية وتنظيمية وتدابير تخص بناء القدرات والتعاون الدولي، وقد جرى في عام 2008 نشر التقرير النهائي الذي تم إعداده من قبل أكثر من 100 خبير، ويعمل الاتحاد الدولي للاتصالات على تنفيذ آلية لوضع إطار مشترك للأمن السيبراني للأمم المتحدة يعالج الأمن السيبراني على المستوى الوطني والإقليمي والدولي.

وتعتبر اتفاقية مجلس أوروبا حول الجرائم السيبرانية (اتفاقية بودابست التي دخلت حيز التنفيذ في 2004) من أهم الاتفاقيات الإقليمية، وتهدف هذه الاتفاقية إلى تنسيق التشريعات الوطنية حول الجرائم السيبرانية وتحسين القدرات الوطنية للتحقيق في هذه الجرائم والتعاون في هذا المجال، وهي تعنى بجمع الأدلة المعلوماتية في مختلف أنواع الجرائم، وليس في الجرائم السيبرانية فقط، وتتضمن الاتفاقية ثلاثة أجزاء: الجزء الأول حول القواعد الموضوعية للجرائم، والجزء الثاني حول إجراءات التحقيق، والجزء الثالث حول آليات التعاون الدولي.

" فعلى مستوى الإتحاد الأوروبي فقد توجهت جهوده في اصدار اتفاقية شاملة تتعلق بجرائم الحاسب الآلي في عام 2000 ، أما السويد فتعد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي إذ صدر قانون البيانات السويدي عام 1973 الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي فضلا عن شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشروع عليها، تعد المملكة المتحدة البريطانية هي أخرى من أولى الدول التي سارعت إلى محاربة الإرهاب الإلكتروني حيث قامت بتحقيقات أولية على يد لجنة القانون الاسكتلندي ضمنتها مذكرة استشارية نشرت عام 1982 وفي عام 1987 ثم إعداد نشاط مماثل أعدته لجنة القانون عام 1988 وقد أسفر عن هذه الأنشطة توصيات وضع بناء عليها قانون إساءة استخدام الحاسب الآلي الذي تمت الموافقة عليه في عام 1990 .

ولتنسيق التشريعات حول جرائم الحاسوب في دول الكومنولث، أعدت مجموعة من الخبراء قانونا نموذجيا في عام 2002 مستوحى من اتفاقية بودابست سمي "قانون الجرائم المتعلقة بالحاسوب"، كما أقر الاتحاد الأوروبي في عام 2003 إطارا قانونيا حول الاعتداءات على الأنظمة المعلوماتية ودخل حيز التنفيذ عام 2005، وقد كانت منظمة التعاون والتنمية في الميدان الاقتصادي أول منظمة دولية أصدرت توجهات حول جرائم الحاسوب وحول أمن أنظمة المعلومات والشبكات وكذلك اعتمدت عام 2014 اتفاقية الاتحاد الإفريقي الخاصة بمجال الأمن السيبراني، وحماية البيانات الشخصية .

ولمكافحة ظاهرة استخدام الإنترنت من طرف المنظمات الإرهابية، أصدر الإنتربول ومركز الأمم المتحدة لمكافحة الإرهاب بشكل مشترك دليلا لمساعدة المحققين على جمع وتحليل وتبادل المعلومات التي يتم العثور عليها عبر الإنترنت ولا سيما على وسائل التواصل الاجتماعي، ويعرض الدليل المعنون باستخدام الإنترنت ووسائل التواصل الاجتماعي للتحقيقات المتعلقة بمكافحة الإرهاب عددا من الممارسات الجيدة في المجالات التالية ويحصر بصورة شاملة أدوات شبكية عملية:

- فهم الطريقة التي يكيف بها الإرهابيون استخدام الإنترنت ووسائل التواصل الاجتماعي لمواصلة الأنشطة على الشبكة.

- الممارسات الجيدة المعتمدة في إجراء التحقيقات عبر الإنترنت لمكافحة الإرهاب.

- الخطوات المتبعة لطلب حفظ الأدلة الإلكترونية وجمعها، بما في ذلك من المزودين بخدمات الإنترنت.

ويقدم الإنتربول المساعدة للبلدان الأعضاء في كشف التهديدات السيبرانية وتصنيفها حسب الأولوية وتنسيق إجراءات التصدي لها المركز المتعدد الاختصاصات المكافحة الجريمة السيبرانية، حيث يضم المركز المتعدد الاختصاصات المكافحة الجريمة السيبرانية خبراء في شؤون الإنترنت من أجهزة إنفاذ القانون والقطاع الخاص لجمع وتحليل جميع المعلومات المتاحة عن الأنشطة الإجرامية المرتكبة في الفضاء السيبراني بهدف تزويد البلدان بمعلومات استخباراتية متسقة يمكن ترجمتها إلى تحرك عملي، وينشر المركز تقارير لتنبيه البلدان إلى تهديدات سيبرانية جديدة وشيكة أو متطورة، وشملت التقارير السابقة التي قدمها المركز تهديدات محددة، ولا سيما برمجيات خبيثة، ورسائل تصيد احتيالي، ومواقع إلكترونية حكومية مخترقة، واحتيال باستخدام أساليب الهندسة الاجتماعية وغير ذلك.

وفي المنطقة العربية تم وضع الاتفاقية العربية في 21 دجنبر 2010 لمكافحة جرائم تقنية المعلومات، والتي تضمنت خمسة فصول أساسية منها فصل خاص بالتجريم ويحدد أنواع الجرائم السيبرانية، وفصل يتعلق بالأحكام الإجرائية، وفصل خاص بالتعاون القانوني والقضائي في ما بين الدول العربية.

ثانيا: على المستوى الوطني

نشير بداية إلى أن القانون 03 ـ 03 المتعلق بالإرهاب يعد أول تشريع مغربي يشير بشكل صريح للإجرام المعلوماتي كوسيلة للقيام بأفعال إرهابية لها علاقة عمدية بمشروع فردي أو جماعي يهدف إلى المساس الخطير بالنظام العام بواسطة التخويف أو الترهيب أو العنف فالفصل 1 ـ 218 حدد بعض الأفعال المجملة على سبيل الحصر ومن بينها الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات، وذلك بعد محاولة تحديد مفهوم الإرهاب في مستهل هذا الفصل .

فقد نص المشرع في بعض الحالات على عقوبات الأفعال الإرهابية في القانون 03 . 03 وفي بعض الحالات الأخرى يحيل إلى تطبيق العقوبات المنصوص عليها في القانون الجنائي وباقي النصوص الخاصة مع تشديدها لذا فقد عمد المشرع بتشديد العقوبة على الجريمة الإرهابية بحيث تحول عقوبة السجن المؤبد إلى الإعدام وتحول العقوبة السجنية ثلاثون سنة إلى السجن المؤبد ويرفع الحد الأقصى للعقوبات الأخرى السالبة للحرية إلى الضعف دون أن تتجاوز ثلاثون سنة إذا كانت العقوبة كما هو منصوص عليه في مجموعة القانون الجنائي وباقي النصوص الخاصة أما إذا كانت العقوبة المقررة للفعل غرامة فيضاعف الحد الأقصى فقط دون الحد الأدنى للغرامة مئة مرة دون أن تقل عن 100.000 درهم.

وفي هذا السياق نشير إلى أنه إذا كان الإرهابيون قد استحدثوا العديد من الطرق لاستخدام الإنترنت في أغراض غير مشروعة، فإن استخدامهم لشبكة الإنترنت يتيح كذلك فرصا لجمع المعلومات الاستخبارية وغير ذلك من الأنشطة الهادفة لمنع الأعمال الإرهابية ومكافحتها، فضلا عن جمع الأدلة من أجل الملاحقة القضائية عن هذه الأعمال، فقدر كبير مما نعرف عن طريقة عمل التنظيمات الإرهابية وأنشطتها وأحيانا أهدافها يستمد من اتصالات المواقع الشبكية ومنتديات الدردشة وغيرها من الاتصالات عبر الإنترنت، وعلاوة على ذلك، فإن زيادة استخدام الإنترنت في أغرا ض إرهابية يتيح زيادة مقابلة في توافر البيانات الإلكترونية التي يمكن جمعها وتحليلها لأغراض مكافحة الإرهاب، وتقوم جهات إنفاذ القانون والمخابرات وغيرها من السلطات باستحداث أدوات تتطور باستمرار للمبادرة إلى منع الأنشطة الإرهابية التي تستخدم فيها شبكة

الإنترنت وكشف هذه الأنشطة وردعها، كما أن استخدام أساليب التحري التقليدية، مثل الموارد المخصصة للترجمة بغرض كشف التهديدات الإرهابية المحتملة في وقت مناسب، أخذ في الازدياد بدوره.

وتتيح المناقشات التي تجرى على الإنترنت فرصة لطرح وجهات النظر المعارضة أو الدخول في نقاش بناء، وهو ما قد يؤدي إلى ثني أنصار محتملين للتنظيمات الإرهابية عن الانخراط في أعمالها، ومن الممكن طرح أفكار مضادة تقوم على أساس راسخ من الحقائق عبر منتديات النقاش والصور وشرائط الفيديو على الإنترنت، كذلك فمن الممكن ضمانا لفعالية الأفكار المطروحة، إظهار التعاطف إزاء القضايا الدفينة التي تساهم في الدفع باتجاه التطرف، مثل الظروف السياسية والاجتماعية، وتسليط الضوء على بدائل التحقيق النتائج المرجوة دون اللجوء للوسائل العنيفة ، كما يمكن بث رسائل استراتيجية تحتوي على أفكار مضادة للدعاية الإرهابية عبر الإنترنت بلغات متعددة للوصول إلى جمهور عريض ومتنوع جغرافيا.

كما يلعب الإعلام دورا مهما في مكافحة الإرهاب وذلك من خلال " تعظيم دور المواطنين في التصدي لجرائم الإرهاب الإلكتروني خاصة ،وأن الجماعات الإرهابية تسعى لاستدراجه وتجنيده لخدمة مصالحها التكوين الثقافي للمواطنين من خلال تمجيد الفضيلة ونبذ كل أنواع الانحراف وضرورة بناء الخطط الإعلامية التي تتمشى مع الواقع الإعلامي والأمني .

ويقدم مركز الاتصالات الاستراتيجية لمكافحة الإرهاب، التابع لوزارة الخارجية في الولايات المتحدة الأمريكية، مثالا على مبادرة مشتركة بين الوكالات، بهدف الحد من التحول إلى التطرف والعنف، بدافع من التطرف عبر الكشف في الوقت المناسب عن أمور في جملتها الدعاية المتطرفة على شبكة الإنترنت والرد السريع عليها بخطاب مضاد محدد الهدف عبر مجموعة واسعة من تكنولوجيات الاتصالات، بما في ذلك الأدوات الرقمية، كما أن المركز يستخدم منصات إعلامية مثل فيسبوك ويوتيوب لبث رسائله المحتوية على خطابات مضادة.

نخلص مما سبق أن الإرهاب السيبراني وليد التطور العلمي الهائل، ويعد من الجرائم المستحدثة، فهو عالمي لا تربطه أي حدود جغرافية، ويمتاز باستغلال التقدم التكنولوجي- بما فيه تكنولوجيا الاتصالات والمعلومات وشبكة الانترنت- من قبل المنظمات الإرهابية بدوافع سياسية، واقتصادية، واجتماعية، من أجل التخطيط، التدريب والتنظيم، لتسهيل ارتكاب الجرائم الإرهابية، بحيث يتعالى مؤشر مخاطره يوم بعد يوم ، مما يستدعي تضافر الجهود الدولية والإقليمية والوطنية لوضع استراتيجية هادفة لمكافحة هذا الخطر الداهم أو التقليل من حدة أثره و ضرره.

لائحة المراجع

الكتب:

- زين العابدين عواد كاظم الكردي، جرائم الإرهاب الإلكتروني (دراسة مقارنة)، منشورات الحلبي الحقوقية، بيروت، ط1 ، 2018 .

- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية الانترنت (الجرائم الالكترونية)، ط1 ، منشورات حلبي الحقوقية، بيروت، 2007 .

- خالد مصطفى فهمي، الحماية القانونية لبرامج الحاسب الآلي في ضوء - قانون حماية الملكية الفكرية طبقا لأحدث التعديلات-، دراسة مقارنة، بدون ناشر ، 2005.

- سعاد إكرام عوض، التزوير المعلوماتي، دراسة نقدية لمختلف القوانين الوضعية، منشأة المعارف، الإسكندرية،

- سهيلة خليل غازي، معوقات التجارة الرقمية في الدول العربية، دار الوفاء لنشر، القاهرة، مصر، 2003 .

- عادل عبد الصادق، استخدام الإرهاب الالكتروني في الصراع الدولي، دار الكتاب الحديث، القاهرة، 2015 .

- عادل عبد الصادق، الإرهاب الالكتروني قوة في العلاقات الدولية نمط جديد وتحديات جديدة، ط1 ، مركز الأهرام للدراسات السياسية والاستراتيجية 2009 .

- علاء الصراط الغامدي، الحرب النفسية للإرهاب الجديد، دار منشاة المعارف، الإسكندرية، مصر،2006 .

- عبادة الحارث خليل قمر، فن الاختزال بين الحقيقة والخيال، جامعة الحسين بن طلال، الأردن، 2015 .

- علي عدنان الفيل، الاج ا رم الالكتروني، مكتبة زين الحقوقية والأدبية، لبنان، ط1 ، 2011 .

- ليندا بن طالب، غسيل الأموال وعلاقتها بمكافحة الارهاب، دراسة مقارنة، دار الجامعة الجديدة لنشر، الإسكندرية، 2011.

- محمد إبراهيم زيد، مقدمة في علم الاجرام وعلم العقاب، دار الهدى للمطبوعات، الإسكندرية، 2008 .

- محمد أقبلي وعابد العمراني : القانون الجنائي المعمق في شروح ـ الطبعة الأولى 2020.

الرسائل والاطروحات

- توفيق شريخي، الإرهاب الالكتروني وتأثيره على أمن الدولة مذكرة مقدمة لنيل شهادة الماستر ، سنة 2017/2018 .

- اسراء طارق جواد، كاظم الجابري، جريمة الإرهاب الالكتروني، دراسة مقارنة، رسالة ماجستير في القانون العام، كلية الحقوق ن جامعة البحرين، العراق،2012 .

- بن صفية وداد، مذكرة مقدمة لنيل شهادة الماستر الأكاديمي تأثير المتغير التكنولوجي على الفواعل الدولية الجديدة للإرهاب الإلكتروني ـ أنموذجا ـ 2018 ـ 2017 .
- حكيم غريب، مكافحة الاشكال الجديدة للإرهاب الدولي، رسالة دكتورة، كلية العلوم السياسية و العلاقات الدولية، جامعة الج ا زئر 03 ، الجزائر ، 2014 .
- عمراني كمال الدين، السياسة الجنائية المنتهجة ضد الجرائم الالكترونية، دراسة مقارنة، أطروحة دكتورة، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان،2012 .
- نجاري بن حاج علي فايزة، الاليات القانونية للإرهاب الالكتروني، مذكرة ماجستير في القانون الدولي لإعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2016 .
- نجاري بن حاج علي فايزة، الآليات القانونية للإرهاب الالكتروني، مذكرة ماجستير في القانون الدولي لإعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2016.

المقالات العلمية

- توفيق مجاهد، طاهر عابسة، جريمة الإرهاب في ضوء احكام الاتفاقية العربية لمكافحة جرائم التقنية المعلومات، لعام 2010 ، مجلة العلوم القانونية والسياسية، المجلد 09 ، العدد 03 ، الجزائر، ديسمبر2018 .
- مايا حسن ملا خاطر، الإطار القانوني لجريمة الإرهاب الإلكتروني، مجلة جامعة الناصر، اليمن، العدد 5، سنة 2015.
- مايا حسن ملا خاطر، الإطار القانوني لجريمة الإرهاب الإلكتروني، مجلة جامعة الناصر، اليمن، العدد 5، سنة 2015.

الجلسة العلمية الثالثة

رئيس الجلسة

الدكتور عبد الرحيم بنبوعيدة

أستاذ التعليم العالي، كلية العلوم القانونية والاقتصادية والاجتماعية – جامعة القاضي عياض مراكش.

المسؤولية الجنائية الناشئة عن جريمة إذاعة الشائعات أو الأخبار الكاذبة عبر وسائل التواصل الاجتماعي في التشريع الجنائي البحريني

الدكتور عبد الباسط محمد سيف الحكيمي
أستاذ القانون الجنائي المشارك بكلية الشريعة والقانون
جامعة صنعاء رئيس قسم القانون الجنائي بكلية الحقوق
جامعة المملكة (البحرين)
E-mail: a.hakimi@ku.edu.bh

بسم الله الرحمن الرحيم

الحمد لله رب العالمين، خلق فسوى، وقدر فهدى، والصلاة والسلام على نبينا محمد، خير من وطىء الثرى، أرسله ربه رحمةً للعالمين ، ففتح به أعيناً عمياً، وآذاناً صماً، وقلوباً غلفاً، وأخرج به البشرية من ظلام الجهل والشرك إلى نور العلم والتوحيد، صلى الله عليه وعلى آله وصحبه ومن اقتفى أثره إلى يوم الدين.

وبعد

لقد برز في الآونة الأخيرة بعض الأنماط الاجرامية التي لم تكن معروفة في الماضي، وكان ظهور هذه الأنماط نتيجة التزاوج بين تكنولوجيا الاتصالات والحاسب الآلي، ومن هذه الأنماط الاجرامية جريمة إذاعة وترويج الشائعات أو الأخبار الكاذبة، وما هذا النمط من الاجرام إلا انعكاس لذلك التزاوج، وتُعد االشائعة أو الأخبار الكاذبة مرضًا اجتماعيًا يتسم بآثار فتاكة، لأن الشائعة تشمل بآثارها الفرد والمجتمع، وتمثل الشائعة المرتكبة إلكترونيًا عبر شبكات وسائل التواصل الاجتماعي انتهاكًا للقوانين النافذة في أي بلد، لأن مستعملي وسائل التواصل الاجتماعي ليسوا جميعهم على خلق قويم، فمنهم من أساء استخدام هذه الوسائل في إذاعة ونشر وترويج سمومه واكاذيبه الهدامة بما فيها ارتكاب الجريمة عبر هذا الوسائل الالكترونية، ولما كانت الشائعات والأخبار الكاذبة المتداولة عبر هذه الوسائل متعددة ومتزايدة، وتطال بآثارها الأمن الوطني والاقتصاد والصحة العامة والنظام العام والسلم الاجتماعي، فقد اتجه المشرع في الدول المختلفة إلى تجريم وعقاب هذا النمط المستحدث من الإجرام وسن التشريعات اللازمة لذلك.

وتُعدُ الشائعة والأخبار الكاذبة من أخطر الوسائل التي تستهدف أمن وسلامة وتآلف المجتمع، كما تستهدف ضرب الأمن أو القطاع الاقتصادي أو الصحي للدولة، فهي تمثل شكلاً من أشكال الحرب النفسية التي تؤثر على الروح المعنوية لأفراد المجتمع، وتكمن الخطورة الكبيرة للشائعة في الوقت الحاضر في سرعة إذاعتها ونشرها وتداولها وسهولة ترويجها عبر وسائل التواصل الاجتماعي سريعة الانتشار والتي أصبحت ميدانًا كبيرًا لإطلاق الشائعات والأخبار الكاذبة، بحيث أضحى من الصعوبة بمكان تحديد مصدرها ومن يقف ورائها، ولقد ازداد تعاظم خطر الشائعة مع تفشي جائحة فيروس COVID 19 وما صاحبها من إذاعة أوترويج للشائعات أو الأخبار الكاذبة ترتب عليها عرقلة السلطات المسؤولة عن مكافحة الجائحة والحد من آثارها المدمرة.

وبناءًا على ذلك فقد وقع اختيارنا للبحث في " المسؤولية الجنائية الناشئة عن إذاعة الشائعات أو الأخبار الكاذبة عبر وسائل التواصل الاجتماعي في التشريع الجنائي البحريني".

أهداف البحث:

يهدف البحث إلى الوقوف على دراسة وتحليل مدى قدرة الوسائل التقليدية على مكافحة الشائعات والتعامل معها ومدى قدرة التشريعات الحالية على ذلك في ظل التطور الهائل والمتسارع في وسائل الاتصالات الحديثة.

تساؤلات الدراسة:

تثير هذه الدراسة العديد من التساؤلات لعل من أهمها:

1- ما الشائعة؟ وما الآثار السلبية الناتجة عنها؟

2- هل تنهض المسؤولية الجنائية عن الشائعة؟ وما هذه المسؤولية وما حدودها؟

3- ما المقصود بجريمة إذاعة الشائعة؟

4- ما العقوبة المقررة لجريمة إذاعة الشائعة؟

اشكالية البحث:

يثير البحث إشكالية مهمة تتمثل في أن العديد من الأفراد لا يدركون ما يقترفوه من جرم بسبب ما يقومون بإذاعته ونشره من أخبار كاذبة أو شائعات وما تسببه من آثار ونتائج سلبية على الوضع الداخلي والبيئة المحيطة.

منهج الدراسة:

سوف نعتمد على المنهج الوصفي والتحليلي في موضوع الدراسة، حيث سنعمد إلى وصف جريمة إذاعة الشائعة ومن ثم تحليل النصوص القانونية الجنائية والآراء الفقهية للوقوف على تحديد اركان الجريمة والمسؤولية الجنائية الناشئة عنها والعقوبة المقررة لها.

خطة الدراسة:

سوف نتناول هذه الدراسة في ثلاثة مباحث هي:

المبحث الأول: مفهوم الشائعة وعلاقتها بوسائل التواصل الاجتماعي.

المبحث الثاني: مفهوم المسؤولية الجنائية الناشئة عن جريمة إذاعة الشائعة أو الأخبار الكاذبة.

المبحث الثالث: العقوبة المقررة لجريمة إذاعة الشائعة أو الأخبار الكاذبة.

الخاتمة.

المبحث الأول: مفهوم الشائعة وعلاقتها بوسائل التواصل الاجتماعي

تمهيد وتقسيم: الحديث عن مفهوم الشائعة ووسائل التواصل الاجتماعي يقتضي منا تقسيم هذا المبحث إلى مطلبين، نبين في أولهما تعريف الشائعة، ونتناول في المطلب الثاني علاقة وسائل التواصل الاجتماعي بالشائعة، وذلك على النحو الآتي:

المطلب الأول: تعريف الشائعة لغة واصطلاحًا:

على الرغم من أن الشائعة قديمة قدم وجود الإنسان على وجه الأرض، وأستخدمت كسلاح في الحروب النفسية وإثارة الفتن، إلا أننا لم نقف على تعريف جامع مانع محدد ودقيق لها، كما أن التشريع البحريني لم يُعرف الشائعة حاله حال التشريعات كافة، إذ لا يعنى المشرع عادة بوضع التعريفات حيث يترك هذه المهمة للفقه والقضاء، وذلك حتى لا يقيد القاضي بتعريف ثم تفضي التغييرات والتطورات إلى تجاوزه فيصبح معيقًا للقاضي في مواجهة الظواهر الإجرامية.

وقد جاء في معجم لسان العرب لإبن منظوربأن الشائعة: مأخوذة من شاع واسم الفاعل شائع، فمادة "شيع" فيقال: شاع الشيب: انتشر، وشاع الخبر: ذاع، والشاعة الأخبار المنتشرة، ورجل شياع: أي لا يكتم سرًا"[101]. وشاع الشيء يشيع، وشع يشعُ شعا وشعاعًا، إذا تفرق. وشاع الشيب شعيًا، وشيعًا وشيوعًا وشيوعة

[101] جمال الدين محمد بن مكرم ابن منظور، لسان العرب، دار صادر، بيروت، ج 10، 1982، ص56.

ومشيعًا، ظهر وتفرق، وشاعت القطرة من اللبن في الماء، وتشيعت، تفرقت. وأشعت به فشاع شيعًا: أي ظهر. والشاعة: الأخبار المنتشرة[102]. والشائعة من شيع: الذيوع والانتشار، واشاعة الخبر: ايصاله إلى سمع كل الناس، وانتشار كلام لا أصل له[103].

ولقد اختلفت وتعددت وتعريفات الشائعة في الاصطلاح باختلاف الزاوية التي يتناول منها الباحث الشائعة، وقد عرفت من الزاوية النفسية بأنها" الترويج لخبر مختلق، لا أساس له من الواقع، أو تعمد المبالغة أو التهويل أو التشويه في سرد خبر فيه جانب ضئيل من الحقيقة، وذلك بهدف التأثير في الرأي العام المحلي أو الاقليمي أو العالمي أو النوعي، تحقيقًا لاهداف سياسية أو اقتصادية أو حربية على نطاق دولة واحدة أو عدة دول، أو النطاق العالمي بأجمعه"[104]. كما عرفت بأنها" معلومات واخبار مغلوطة قابلة للانتشار عبر الشبكات، لها تأثيرات صادمة"[105].

ويمكننا تعريف الشائعة الإلكترونية بأنها إذاعة وترويج الأخبار الكاذبة أو المضللة عن دولة أو شخص أو حدث ما بأية وسيلة الكترونية بهدف التأثير في جمهور المتلقين والحاق الضرر بأمن الدولة أو جيشها أو اقتصادها أو نظامها الصحي.

المطلب الثاني: علاقة وسائل التواصل الاجتماعي بالشائعة:

تتعدد الوسائل الإكترونية التي تقترف جريمة إذاعة الشائعة والأخبار الكاذبة عبرها، وهي ما اصطلح على تسميتها شبكات ومواقع التواصل الاجتماعي. وتعرف وسائل التواصل الاجتماعي بأنها" الوسائل التقنية الحديثة التي يستخدمها الأشخاص فيما بينهم لتحقيق التواصل الاجتماعي المشاع عبر شبكة الانترنت كالفيسبوك، تويتر، اليوتيوب، وغيرها"[106]، كما عرف المشرع الفرنسي في المادة (4) من القانون رقم 555 – 2004 التواصل الاجتماعي عبر شبكة الإنترنت بأنه بروتوكول اتصال مفتوح، أو ربط بيانات وتبادلها بأي شكل يصل

---

[102] محمد مرتضى الحسيني الزبيدي، تاج العروس من جواهر القاموس، تحقيق مجموعة من المحققين، دار الهداية، باب العين المهملة، مادة شيع، (5356/1).

[103] د. محمد روا قلعه جي ود. حامد صادق قنيبي، معجم لغة الفقهاء، دار النفائس للطباعة والنشر بيروت، لبنان، ط1، 1988، ص68.

[104] د. عباس الحسني، علم النفس العسكري، ج1، مطبعة الرشاد، بغداد، 1968، ص155.

[105] Rudat,A. Twitter Spreads Rumors: Influencing Factors on Twitter's Role in Rumor Spread Among University Students, PhD Thesis, Tubingen: Tubingen> 2015, p 2.

[106] د. سلمان بن عبدالله بن حمود أبا الخيل، مقومات المواطنة الصالحة، نص محاضرة القاها في جامع الامام تركي بن عبدالله بالرياض. منشورة على موقع: http://islamancient.com/ressources/docs/366.pdf.
تاريخ الولوج 2021/7/4.

إلى الجمهور دون قيد على أي محتوى تبادلي من قبل مقدمي الخدمات التقنية[107]، بينما عرف المشرع الإماراتي الموقع الإلكتروني بأنه " مكان إتاحة المعلومات الإلكترونية على الشبكة المعلوماتية، ومنها مواقع التواصل الاجتماعي، والصفحات الشخصية والمدونات"[108].

وأبرز وسائل التواصل الاجتماعي تتمثل في الفيسبوك، تويتر، الواتس أب، اليوتيوب، وغيرها، وسوف نقصر التعريف على أهم مواقع التواصل الاجتماعي في الآتي.

1- الفيسبوك (Facebook):

الفيسبوك هو عبارة عن شبكة تواصل اجتماعي يتم الدخول إليها واستعمالها بصورة مجانية، وتدار من قبل شركة فيسبوك ذات المسؤولية المحدودة، وبامكان المستخدمين الإنضمام إلى صفحات خاصة بجهات العمل أو الجامعة أو النادي أو النقابة بما يحقق التواصل مع الآخرين والتفاعل معهم، كما يمكن لمن لديه صفحة في الفيسبوك إضافة أصدقاء وإرسال طلبات الصداقة أو الرسائل إليهم. وقد أطلق الموقع الالكتروني فيسبوك في شباط فبراير 2004 واتيح لطلبة جامعة هارفرد نشر صورهم الخاصة بالاضافة إلى نشر تفاصيل أخرى متعددة عن الطلاب مثل جداولهم الدراسية والنوادي التي ينتمون إليها، وبشكل سريع انتشرت شعبية الموقع وسمح لطلاب جامعات أخرى مثل جامعة ييل وستانفورد الانضمام إلى المنصة الجديدة، وفي عام 2006 فتحت المنصة أبوابها أمام الجمهور ممن يبلغ 13 عامًا فأكثر، ممن لديهم عنوان بريد الكتروني، ويرتاد الموقع حاليًا أكثر من مليار شخص سنويًا[109]،

وتُعد هذه الشبكة من أكثر الشبكات الالكترونية إستخدامًا وفيها تنتشر الشائعات والأخبار الكاذبة والمضللة على نطاق واسع، وتستهدف تلك الشائعات مهاجمة دول أو أفراد وتؤثر بشكل كبير على الناس الذين قد يستجيبون لما يذاع عبرها من شائعات وأكاذيب تلحق الأضرار بالأمن الوطني أو الاقتصاد الوطني أو القوات العسكرية للدول أو النظام الصحي لها.

---

[107] صدر هذا القانون في 21 يونيو 2004.

[108] المادة (1) من المرسوم بقانون رقم (5) لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات.

[109] محمد مروان ، تعريف الفيسبوك، منشور على موقع الويب .

https://mawdoo3.com/.2021/7/4 تاريخ الولوج

/ تاريخ الولوج 2021/7/4https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide

وينظر كذلك د. دنيا عبدالعزيز فهمي، الحماية الجنائية من إساءة استخدام مواقع التواصل الاجتماعي- دراسة مقارنة، دار النهضة العربية، 2018، 26.

2- تويتر (Twitter):

يعتبر تويتر من أهم مواقع شبكة التواصل الاجتماعي، وتم انشاؤه في 2006 وهو يقدم خدمة تدوين مصغر يسمح لمستخدميه نشر تغريدات قصيرة بحد أقصى 140 حرف في التغريدة الواحدة[110]. وشبكة تويتر تُعد من الشبكات واسعة الانتشار في وقتنا الحاضر وتنشر فيها الأخبار والتغريدات التي قد تتضمن إذاعة شائعات أو أخبار كاذبة تؤثر على نفسيات الناس وضعف من معنوياتهم أو ثقتهم في الأمن أو الاقتصاد أو جيشهم أو نظامهم الصحي.

3- يوتيوب (YouTube):

تأسس موقع يوتيوب في 2005 ويعتبر من مواقع شبكات التواصل الاجتماعي، وهو من أشهر المواقع العالمية والأكثر استخدامًا، ويتبع شركة جوجل، وهو موقع متخصص بمقاطع الفيديو المجانية، والتي يقوم المستخدمين بنشرها ومشاهدتها[111].

ومن القواعد الملزمة للنشر على هذا الموقع أنه لا يسمح للمستخدمين للموقع نشر أي فيديو أو مشاركة أفلام لها حقوق نشر محفوظة وكذلك نشر أفلام ذات محتوى إباحي أو التي تسيء لشخصية معينة أو الافلام التي تشجع على الارهاب أو الاجرام[112]. وكثيرًا ما يستخدم اليوتيوب في إذاعة الشائعات أو الأخبار الكاذبة عبر الفيديوهات التي يقوم المستخدمون بنشرها عبر هذا الموقع، وقد لاحظنا كيف تبث الكثير من الفيديوهات السلبية والتي يذاع عبرها أخبار كاذبة أو شائعات حول فيروس كورونا المستجد، وكيف أدت تلك الشائعات إلى تأخير وعرقلة جهود السلطات المختصة بمكافحة الفيروس، وكذلك ما يبث عبر هذا الموقع من فيديوهات تتضمن أخبار كاذبة وشائعات حول أوضاع البلد وهو ما يؤثر سلبًا على سمعته في الخارج، وما يبث عبره ايضًا من أخبار كاذبة أو شائعات عن شخصيات معينة تؤدي إلى الحط من اعتبارهم بين جمهور المتلقين.

---

[110] تسنيم معابرة ، أهم مواقع التواصل الاجتماعي، منشر على موقع الويب .

https://mawdoo3.com/. تاريخ الولوج 2021/7/4. وينظر د.دنيا عبدالعزيز فهمي، مرجع سابق، ص27.

[111] المرجع السابق ذاته .

https://mawdoo3.com/. تاريخ الولوج 2021/7/4.

[112] المرجع السابق ذاته .

https://mawdoo3.com. تاريخ الولوج 2021/7/4.

المبحث الثاني: مفهوم المسؤولية الجنائية الناشئة عن جريمة إذاعة الشائعة أو الأخبار الكاذبة الكترونيًا

تمهيد وتقسيم: سوف نخصص هذا المبحث لدراسة المسؤولية الجنائية من حيث تعريفها وعناصرها ثم نعرج على أركان جريمة الشائعة الالكترونية، وهو ما يقتضي تقسيم المبحث إلى ثلاثة مطالب، نتناول في الأول تعريف المسؤولية الجنائية، ونبين في الثاني أساس المسؤولية الجنائية وعناصرها ، ونفرد الثالث لدراسة أركان جريمة إذاعة الشائعة الكترونيًا..

المطلب الأول: تعريف المسؤولية الجنائية الناشئة عن جريمة إذاعة الشائعة أو الأخبار الكاذبة:

عرفت المسؤولية الجنائية لغة بأنها المطلوب الوفاء به، وتعني المحاسبة عنه وهي تطلق بصفة عامة على حال أو صفة من يسأل عن أمر تقع عليه تبعته، يقال أنا برىءٌ من مسؤولية هذا العمل، وتطلق أخلاقياً على : التزام الشخص عما يصدر عنه قولاً أو عملاً، كما تطلق قانوناً على الالتزام بالخطأ الواقع على الغير طبقاً للقانون[113].

أما في الفقه فقد تعددت التعريفات حيث عرفها بعضهم بأنها صلاحية الشخص لتحمل العقوبة التي يقررها القانون كأثر للجريمة التي ارتكبها[114]. غير أن هذا التعريف أغفل بيان العلاقة بين الفرد والسلطة في حين تلك العلاقة تعد جوهر المسؤولية الجنائية. فالمسؤولية هي أهلية الشخص لتحمل الجزاء الذي يقرره قانون العقوبات. وعرفها آخر بأنها "الالتزام بتحمل النتائج القانونية المترتبة على توافر أركان الجريمة، وموضوع هذا الالتزام هو العقوبة أو التدبير الاحترازي الذي ينزله القانون بالمسؤول عن الجريمة"[115].

ويمكننا تعريف المسؤولية الجنائية الناشئة عن جريمة إذاعة وترويج الشائعة أو الأخبار الكاذبة عبر وسائل التواصل الاجتماعي، بأنها تحمل الناشر أو المروج النتائج القانونية المترتبة عن الشائعة التي أذاعها أو روجها في أحد مواقع التواصل الاجتماعي، وخضوعه للعقاب المقرر لها قانوناً. فارتكاب الشخص لجريمة إذاعة الشائعة الكترونيًا يثير فكرة المسؤولية الجنائية، وتوقيع الجزاء الجنائي عليه بمقتضى حكم قضائي، يعني ثبوت المسؤولية الجنائية قبله.

---

[113] مجمع اللغة العربية، مصر، المعجم الوسيط، مكتبة الشروق الدولية ج1،ط4، باب السين،411،2004.

[114] د. محمد أبو زهرة، الجريمة والعقوبة في الفقه الإسلامي، دار الفكر العربي، القاهرة، بدون، ص110.

[115] د. محمود نجيب حسني، شرح قانون العقوبات – القسم العام اللبناني، المجلد الأول، مشورات الحلبي الحقوقية، ط3، بدون سنة نشر،463.

المطلب الثاني: أساس المسؤولية الجنائية وعناصرها:

الفرع الأول: أساس المسؤولية الجنائية:

لا شك أن المسؤولية الجنائية الناشئة عن اقتراف الشخص لجريمة إذاعة الشائعة أو الأخبار الكاذبة الكترونيًا عبر وسائل التواصل الاجتماعي تعني تحـمل الجاني تبعة الآثار الجرمية الناتجة عن سلوكه الإجرامي، ولكي يكون الشخص أهلاً لتحمل تبعة إذاعة الشائعة أو الأخبار الكاذبة لابد أن يكون متمتعًا بالأهلية الجنائية عند اقتراف ذلك السلوك، أي أن يكـــون مدركاً مختاراً له عند إتيانه، ولذلك يوصف القصد الجنائي كصورة من صور الركن المعنوي للجريمة العمدية بأنه ركن المسؤولية الجنائية، ويبرر ذلك بأن القصد الجنائي يفترض توافر الركنين الشرعي والمادي للجريمة، ومـــن ثم إذا توافر دل ذلك على إجتماع كل اركان الجريمة العمدية، مما يقتضي القول بقيام المسؤولية الجنائية، كما يـــبرر ذلك بأن توافر القصد الجنائي يفترض توافر الأهلية الجنائية، إي الأهلية للمسؤولية الجنائية العمدية، ولكن هذه الأهلية تنهض على المسؤولية الجنائية[116].

وقد تنازع تحديد أساس المسؤولية الجنائية مذهبان، أحدهما يقوم على أساس حرية الاختيار، وهي القدرة على المفاضلة بين الدوافع المختلفة ومن ثم توجيه الإرادة وفقًا لأحدها، فهي قدرة الجاني على سلوك الطريق الذي يتفق مع القانون أو الطريق المخالف له وتفضيله الطريق الأخير. وتقاس هذه القدرة على أساس استطاعة مقاومة الدوافع التي تغري بسلوك طريق الجريمة، فإن توافرت هذه الاستطاعة لدى الجاني، غير أنه أراد عدم استعمالها فانقاد لهذه الدوافع فهو حر في اختياره ومسؤول عما اختار، وبقدر ما تنقص هذه الاستطاعة يقل نصيبه من الحرية وحظه من المسؤولية تبعاً لذلك[117].

بينما ثانيهما وهو مذهب الجبرية، ويرى أنصاره أن أفعال الإنسان، بوصفها ظواهر طبيعية نفسية، خاضعة لجملة من القوانين التي تحكم ظواهر الكون على نحو لازم، فهي على هـــذا النحو نتيجة حتمية لأسباب مؤدية إليها. فالجريمة ليست ثمرة حرية الاختيار ولكنها ثمرة نوعين من العوامل، داخلية تكوينية وخارجية بيئية اجتماعية، مما يعني أن حرية الاختيار لا وجود لها، وانما هي وليدة الجهل بأسباب الجريمة الحقيقية[118].

---

[116] د. محمود نجيب حسني، شرح قانون العقوبات – القسم العام، دار النهضة العربية، القاهرة، 1989، ص504.

[117] د.محمد مصطفي القللي، في المسؤولية الجنائية، مطبعة عبدالله وهبة، مصر، 1945، ص5.

[118] د. محمود نجيب حسني، المرجع السابق، ص 107 ، 108.

وقد أخذ المشرع البحريني بالمذهب الأول مؤسسًا المسؤولية الجنائية على أساس حرية الاختيار[119]، ولذلك فالمسؤول جنائيًا عن جريمة إذاعة الشائعة أو الأخبار الكاذبة هو الشخص الذي يتمتع بملكتي الادراك وحرية الاختيار عند اقتراف الجريمة، ومن ثم فالجاني الذي يتعمد إذاعة الشائعة أو الأخبار الكاذبة عبر وسائل التواصل الاجتماعي تقوم مسؤوليته الجنائية عن كافة النتائج المترتبة عن سلوكه الإجرامي الذي اقترفه طالما أنه كان متمتع بحرية الاختيار والادراك عند اقترافه.

الفرع الثاني: عناصر المسؤولية الجنائية:

لكي تنهض المسؤولية الجنائية قبل مرتكب جريمة إذاعة الشائعة أو الأخبار الكاذبة عبر وسائل التواصل الاجتماعي لابد من توافر عنصرين أولهما الإدراك وثانيهما الإرادة.

أ- الادراك: ويقصد به قدرة الشخص على فهم ماهية السلوك وطبيعته وتوقع الآثار المترتبة عليه، وتنصرف هذه القدرة إلى ماهية الفعل وطبيعته وتوقع آثاره، كما أنها تتصل بعناصر الفعل وخصائصه وتنصرف ايضاً إلى خطورته على المصلحة أو الحق الذي يحميه القانون وما توحي به من اعتداء على ذلك الحق[120]، ولا تنصرف القدرة على الفهم إلى التكييف القانوني للفعل، فالتمييز يعدُ متوافراً ولو ثبت أنه لم يكن في استطاعة المتهم العلم بهذا التكييف، فالعلم بقانون العقوبات والتكييف المستخلص منه مفترض في حق الكافة[121]. وبناءً عليه يتعين لقيام المسؤولية الجنائية لمن يرتكب جريمة إذاعة الشائعة أو الأخبار الكاذبة عبر وسائل التواصل الاجتماعي أن يكون مدركاً لماهية السلوك الذي اقدم عليه وخالف به النصوص التجريمية المقررة في قانون العقوبات وترتبت على سلوكه النتائج التي حددها المشرع في نصوص القانون العقابي.

ب- الإرادة: ويقصد بها حرية الاختيار، وهي صفة تخصص الممكن فهي نشاط نفسي يستند إليها الإنسان في التأثير على ما حوله من أشخاص وأشياء، ومن ثم فهي توجه القوى العصبية لإتيان أفعال تفضي إلى آثار مادية مما يشبع بها الإنسان حاجاته، والإرادة بهذا المعنى تفترض العلم وتستند إليه، فهي لذلك نشاط يتولد عن وعي[122] ، والإرادة هي مقدرة الجاني على تحديد الوجهة التي

---

[119] تنص المادة (31):"لا مسؤولية على من ارتكب الفعل المكون للجريمة من غير إدراك أو اختيار".

[120] د. محمود نجيب حسني، القسم العام اللبناني، مرجع سابق، ص662.

121 تنص المادة (29) من قانون العقوبات البحريني على أنه: " لا يقبل الاحتجاج بجهل أحكام هذا القانون.....".

[122] د. فخري عبدالرزاق الحديثي، شرح قانون العقوبات – القسم العام، مكتبة السنهوري، بيروت، لبنان، 2018، ص 305.

تتخذها إرادته، أي مقدرته على دفع إرادته في وجهة بعينها من الوجهات المتعددة التي يمكنه أن يتخذها، ولكن هذه الحرية مقيدة بعوامل لا يمكن للجاني السيطرة عليها، وهناك مجال يتمتع في داخله بحرية الاختيار، والقانون هو من يحدد هذا المجال، فإن انتفى أو ضاق على نحو معتبر انتفت حريته في الاختيار[123]، وامتنعت مسؤوليته الجنائية. والعوامل التي تقيد حرية الاختيار قد تكون خارجية مثل الإكراه والضرورة وقد تكون داخلية نفسية أو عقلية[124].

ولذلك لا يكفي أن يكون الإنسان قادرًا على أن يعلم الوجهات المختلفة التي يمكن أن تتخذها إرادته وانما يجب أن تكون المقدرة على انتفاء الوجهة التي يمكن أن تتخذها إرادته، ولذا يفترض لوجودها أن يكون الجاني حرًا في تصرفاته غير مكره عليها وفي وضع جسدي ونفسي وعقلي يساعده على اتخاذ التصرفات التي يريدها.

وتأسيسًا على ما سبق تنهض المسؤولية الجنائية لمرتكب جريمة إذاعة الشائعة أو الأخبار الكاذبة إذا كان قد ارتكب الجريمة وهو مدرك لماهية السلوك الذي أقدم عليه وكان حرًا مختارًا لحظة اقترافه، أي خاليًا من عيوب الإدراك و الإرادة.

المطلب الثالث: اركان جريمة إذاعة الشائعة أو الأخبار الكاذبة:

ان جريمة إذاعة الشائعة أو الأخبار الكاذبة أو ترويجها تنهض على ثلاثة أركان هي: الركن الشرعي، الركن المادي، والركن المعنوي. وإذا كان الفقه متفق على الركنين المادي والمعنوي، إلا أنهم أختلفوا حول الركن الشرعي، فالبعض يقول بالركن الشرعي والبعض ينكر ذلك على أساس أن النص الجنائي هو من خلق الجريمة عملًا بمبدأ الشرعية الموضوعية" لا جريمة ولا عقوبة ولا تدبير إلا بناءً على قانون"، ومن ثم لا يجوز أن يكون الخالق عنصرًا فيما خلق. ولكن طالما وأن بحثنا يتعلق بجريمة إذاعة وترويج الشائعة أو الأخبار الكاذبة عبر مواقع التواصل الاجتماعي فحري بنا أن نشير إلى النصوص القانونية التي جرمت هذه الجريمة وقررت العقاب عليها.

الفرع الأول: الركن الشرعي لجريمة إذاعة الشائعة أو الأخبار الكاذبة:

يتمثل الركن الشرعي في النصوص التي بموجبها جرم المشرع إذاعة الشائعة أو الأخبار الكاذبة سواء في قانون العقوبات الأساسي أم في قانون العقوبات التكميلي. وحيث أن المشرع البحريني أورد نصوصًا في قانون

---

[123] د.محمود نجيب حسني، اللبناني، المرجع السابق، ص262-663.

124 راجع على سبيل المثال المواد (31، 33، 35) من قانون العقوبات البحريني.

العقوبات جرم بموجبها إذاعة الشائعة أو الأخبار الكاذبة وأحال في المادة (23) من قانون جرائم تقنية المعلومات رقم (60) لسنة 2014 إلى القوانين الأخرى بالنسبة للجرائم المنصوص عليها فيها إذا ارتكبت بواسطة نظام[125] أو أية وسيلة تقنية معلومات[126] يعاقب بالعقوبة المقررة لتلك الجريمة فإننا سوف نتناول هذه الجريمة في قانون العقوبات وفي نطاق قانون الصحافة البحريني.

اولًا: في نطاق قانون العقوبات البحريني رقم (15) لسنة 1976: وردت العديد من النصوص التي جرمت إذاعة الشائعة أو الأخبار الكاذبة، ولعل من أهم تلك النصوص في هذا القانون، نص المادة (168) والتي قررت بأنه:"يعاقب بالحبس مدة لا تزيد على سنتين وبالغرامة التي لا تتجاوز مائتي دينار أو بإحدى هاتين العقوبتين من أذاع عمدًا أخبارًا كاذبة مع علمه بأنها من الممكن أن تحدث ضررًا بالأمن الوطني أو بالنظام العام أو بالصحة العام، متى ترتب على ذلك حدوث الضرر. ويشترط في الأخبار الكاذبة والمتعلقة بإحداث الضرر بالأمن الوطني المنصوص عليها في الفقرة السابقة أن تكون تحريضًا على العنف، أو من شأنها أن تحرض على العنف، وعلى أن يكون بينها وبين حدوث ذلك العنف أو احتمالية حدوثه رابط مباشر". من خلال هذا النص نلاحظ أن المشرع لم يشر بشكل صريح إلى لفظ الشائعة ولكن الشائعة كما ذكرنا سابقًا ما هي إلا أخبار كاذبة يتم نشرها وترويجها ويترتب عليها ضرر بالأمن أو بالنظام العام أو بالصحة العامة، مثل إذاعة وترويج الشائعات عن لقاح فيروس كورونا المستجد وما يترتب عليها من ضرر بالغ بالصحة العامة لما توقعه في نفوس الناس من مخاوف لا أساس لها من اللقاح مما يفضي إلى عزوف الناس عن التطعيم، ومن ثم انتشار الفيروس وما ينجم عن ذلك من مخاطر وأضرار صحية وخسائر اقتصادية جسيمة، وهذه الجريمة لا تقع الا عمدية، ويشترط لاستحقاق العقاب على جريمة إذاعة الشائعة أو الأخبار الكاذبة المتعلقة بإحداث الضرر بالأمن الوطني أن تكون الاخبار الكاذبة والشائعات تتضمن في طياتها تحريضًا على العنف أو من شأنها أن تحرض على العنف، وأن تقوم الرابطة السببية المباشرة بين تلك الاخبار الكاذبة وبين ذلك العنف أو احتمالية حدوثه.

بينما تحدثت المادة (133) عقوبات عن جريمة إذاعة أخبار أو بيانات أو إشاعات كاذبة أو مغرضة أو دعاية مثيرة في زمن الحرب، وكان من شأنها إلحاق الضرر بالاستعدادات الحربية للدفاع عن دولة البحرين أو

---

[125] **عرفت المادة (1) من قانون جرائم تقنية المعلومات نظام تقنية المعلومات بأنه:"أداة أو مجموعة أدوات متصلة أو ذات صلة ببعضها، ويقوم وأحد منها أو أكثر بمعالجة آلية لبيانات وسيلة تقنية المعلومات وفقًا لبرنامج".**

[126] **عرفت المادة (1) من قانون جرائم تقنية المعلومات وسيلة تقنية المعلومات بأنها:"أي أداة أو وسيلة إلكترونية أو مغناطيسية أو بصرية أو كهروكيميائية أو أية أداة تدمج بين تقنيات الاتصال والحوسبة أو أية أداة أخرى لديها القدرة على استقبال أو إرسال البيانات ومعالجتها وتخزينها واسترجاعها بسرعة فائقة".**

بالعمليات الحربية للقوات المسلحة أو أثار الفزع بين الناس أو إضعاف الجلد في الأمة، حيث نصت هذه المادة على أنه:"يعاقب بالسجن مدة لا تزيد على عشر سنوات من أذاع عمدا في زمن الحرب أخبار أو بيانات أو إشاعات كاذبة أو مغرضة أو عمد إلى دعاية مثيرة وكان من شأن ذلك إلحاق الضرر بالاستعدادات الحربية للدفاع عن دولة البحرين أو بالعمليات الحربية للقوات المسلحة أو أثار الفزع بين الناس أو إضعاف الجلد في الأمة.

وتكون العقوبة السجن إذا ارتكبت الجريمة نتيجة التخابر مع دولة أجنبية.

وتكون العقوبة السجن المؤبد إذا ارتكبت الجريمة نتيجة للتخابر مع دولة معادية".

ويلاحظ على هذا النص أنه اشترط أن تكون إذاعة الاخبار أو البيانات أو الإشاعات الكاذبة قد ارتكبت في الداخل أو في الخارج وفي زمن الحرب، وأن يترتب عليها احتمالية الحاق الضرر بالاستعدادات الحربية أو بالعمليات الحربية أو إثارة الفزع بين الناس أو إضعاف معنويات الأمة، كما أن العقوبة تشدد لتصبح السجن بحد أقصي لا يزيد على 15 سنة إذا وقعت الجريمة نتيجة التخابر مع دولة أجنبية، وتشدد العقوبة إلى السجن المؤبد إذا ارتكبت الجريمة نتيجة التخابر مع دولة معادية للبحرين.

في حين نصت المادة (134) عقوبات بحريني على أنه:" يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبالغرامة التي لا تقل عن مائة دينار أو بإحدى هاتين العقوبتين كل مواطن أذاع عمدا في الخارج أخبارا أو بيانات أو إشاعات كاذبة أو مغرضة حول الأوضاع الداخلية للدولة وكان من شأن ذلك إضعاف الثقة المالية بالدولة أو النيل من هيبتها أو اعتبارها، أو باشر بأية طريقة كانت نشاطا من شأنه الإضرار بالمصالح القومية.

وتكون العقوبة السجن مدة لا تزيد على عشر سنوات إذا وقعت الجريمة في زمن الحرب".

وقد شددت المادة (142) من قانون العقوبات البحريني عقوبة هذه الجريمة بحيث أجازت الحكم بالإعدام متى كان قصد الجاني من الجريمة إعانة العدو أو الإضرار بالعمليات الحربية للقوات المسلحة وكان من شأنها تحقيق الغرض المذكور، وهنا نلاحظ أن المشرع اشترط وقوع الضرر الفعلي.

ثانيًا: في نطاق قانون الصحافة والطباعة والنشرالبحريني رقم (47) لسنة 2002: عرف قانون الصحافة المطبوعات في المادة (3) منه بقوله:" الكتابات أو الرسوم أو المؤلفات المغناة أو الصور أو وعاء المنتجات السمعية أو السمعية البصرية أو غيرها من وسائل التعبير مما هو مطبوع أو مرسوم أو مصور أو مسجل بأية

طريقة من الطرق بما فيها الطرق الإلكترونية أو الرقمية، أو مما هو قابل للثبوت على دعامة، أو محفوظ في أوعية حافظة ممغنطة، أو إلكترونية، أو أية وسيلة تقنية جديدة متى كانت معدة وقابلة للتداول".

كما جرم القانون ذاته نشر الأخبار الكاذبة وعاقب عليها بعقوبة الغرامة التي لا تزيد على الفي دينار في المادة (70) التي تنص على أنه:" مع عدم الإخلال بأية عقوبة أشد ينص عليها قانون العقوبات أو أي قانون آخر، يعاقب بالعقوبة المنصوص عليها في المادة السابقة على نشر ما يتضمن:

أ) عيباً في حق ملك أو رئيس دولة عربية أو إسلامية، أو أية دولة أخرى تتبادل مع مملكة البحرين التمثيل الدبلوماسي.

ب) إهانة أو تحقيراً لأي مجلس تشريعي أو المحاكم أو غيرها من الهيئات النظامية.

ج) نشر أخبار كاذبة أو أوراق مصطنعة أو مزورة مسندة بسوء نية إلى الغير متى كان من شأن هذا النشر تكدير الأمن العام أو إلحاق ضرر بمصلحة عامة.

د) نشر أنباء عن الإتصالات الرسمية السرية، أو بيانات خاصة بقوة الدفاع يترتب على إذاعتها ضرر للصالح العام، أو إذا كانت الحكومة قد حظرت نشرها، وتضاعف العقوبة إذا ارتكبت الجريمة في وقت الحرب أو أثناء تعبئة عامة أو جزئية لقوة دفاع البحرين. ولا يجوز اتخاذ الإجراءات الجنائية في الحالات المنصوص عليها في البند (ب) من هذه المادة إلا بناء على طلب رئيس الهيئة أو الجهة ذات الشأن".

من خلال النصين السابقين نجد أن المشرع البحريني قد جرم نشر الأخبار الكاذبة (الشائعات) أو أوراق مصطنعة أو مزورة مسندة بسوء نية إلى الغير إدا كان من شأن النشر تكدير الأمن العام أو إلحاق ضرر بمصلحة عامة، وسواء وقع النشر بوسيلة ورقية أم بوسيلة إلكترونية عبر مواقع التواصل الاجتماعي.

ثالثًا: في نطاق قانون جرائم تقنية المعلومات رقم (60) لسنة 2018: لم ينص هذا القانون بشكل صريح عن جريمة إذاعة الشائعة والأخبار الكاذبة، ولكن إذا ارتكبت هذه الجرائم الكترونيًا بواسطة مواقع التواصل الاجتماعي فقد أحالت المادة (23) من هذا القانون إلى الجرائم المنصوص عليها في القوانين الأخرى إذا ارتكبت بواسطة نظام أو وسيلة تقنية معلومات، إذ نصت هذه المادة على أنه:" فيما عد ما ورد بشأنه نص خاص في هذا القانون، من قام بارتكاب جريمة منصوص عليها في قانون آخر بواسطة نظام أو أية وسيلة تقنية معلومات، يعاقب بالعقوبة المقررة لتلك الجريمة".

من خلال نص هذه المادة إذا ارتكبت جريمة إذاعة الشائعات أو الأخبار الكاذبة الكترونيًا عبر وسيلة من وسائل التواصل الاجتماعي فإنه يعاقب بالعقوبة المقررة للجريمة في القانون الذي ورد النص عليها فيه. وهكذا يتضح لنا أن اقتراف جريمة الشائعة عبر وسائل التواصل الاجتماعي تخضع لمبدأ الشرعية، ويتحقق بذلك الركن الشرعي للجريمة.

الفرع الثاني: الركن المادي

يتمثل الركن المادي في جريمة إذاعة وترويج الشائعة أو الأخبار الكاذبة عبر مواقع التواصل الاجتماعي في المظهر الخارجي لها، وهو السلوك الايجابي الصادرعن إنسان سواء باليد كالكتابة أو بالرسم أو الاشارة أو بالفم على شكل قول أو صوت أو تسجيل ونحو ذلك[127] إذا ما تم هذا السلوك الاجرامي عبر موقع التواصل اجتماعي المختلفة، أو السلوك السلبي عندما يمتنع الجاني عن القيام بعمل يستطيع القيام به لمنع إذاعة أو نشر الشائعات والأخبار الكاذبة بشرط أن يكون هناك واجب قانوني يلزمه بالقيام بذلك العمل الذي أمتنع عن القيام به ووقوع النتيجة المترتبة على ذلك الامتناع، فهو قوام الجريمة المادي المتمثل بالسلوك الحقيقي الذي تترتب عليه نتيجة إجرامية[128].

إذن الركن المادي هو سلوك سلبي أو إيجابي ونتيجة إجرامية مترتبة على السلوك والتي قد تتمثل بالضرر الذي لحق الحق أو المصلحة التي يحميها القانون أو إحتمال إلحاق الضرر بها، ولابد من قيام علاقة سببية مباشرة بين السلوك والنتيجة الإجرامية. وسوف نتحدث هنا عن السلوك الاجرامي والنتيجة الاجرامية والشروع في الجريمة.

اولًا: السلوك الاجرامي

فالسلوك قد يتمثل في إذاعة إشاعات أو أخبار أو بيانات كاذبة أو مغرضة أو دعاية مثيرة والإذاعة تشمل الترويج لأن الترويج وسيلة لإذاعة الشائعات والأخبار الكاذبة أو المغرضة، فما هو المقصود بالإذاعة والترويج؟

1: إذاعة أخبار أو بيانات أو إشاعات كاذبة أو مغرضة: ويقصد بإذاعة الأخبار أو البيانات أو الإشاعات الكاذبة نشر الأخبار المغايرة للحقيقة وإظهار الأشياء على غير حقيقتها، فالجاني هنا يقوم باستخدام وسائل التواصل الاجتماعي لنشر وإعلان وبث وإفشاء وإظهار الأخبار أو البيانات خلافًا للحقيقة بغرض التأثير بالمستهدف من تلك الأخبار أو البيانات الكاذبة وغير الحقيقية.

---

[127] د.علي حسن الشرفي، أحكام الشائعات في القانون العقابي المقارن، بحث مقدم إلى مؤتمر أساليب مواجهة الشائعات، أكاديمية نايف للعلوم الأمنية – الرياض- 2001، ص141.

[128] د.محمود نجيب حسني، القسم العام -1989، مرجع سابق، ص280.

ولذلك فالخبر الكاذب أو المغرض يكون كاذبًا أو مغرضا عندما لا يطابق الحقيقة كلها أو جزء منها سواء كان عن طريق الحذف أو الإضافة أو سوى ذلك من الوسائل التي تناقض الحقيقة في أية صورة من صورها.

والإشاعة الكاذبة أو المغرضة تكون كذلك عندما تكون هناك رواية عن وقائع بأسلوب يشعر المتلقي بأن ما يذاع أو ينشر عبر وسائل التواصل الاجتماعي هو علم عام معروف للجمهور، أي هي رواية عن أمر أو حدث أو شخص بأسلوب يشعر بالذيوع والانتشار لما ينشر أو يذاع، فهي نوع من الخبر غير المؤكد، ويريد قائله أو ناشره أو مذيعه إلفات النظر إلى تأكيده وعلم الناس به[129].

2: إذاعة دعاية مثيرة أو أخبار مغرضة: يقصد بالدعاية المثيرة تلك الحملات المدبرة لإثارة الشعور بالهلع وبث الخوف والذعر بين الناس، والتي هي في جوهرها معلومات تثير في النفس نوعًا من القلق أو الاضطراب، يفسد على صاحبه ملكة الحكم على الأشياء أو الأشخاص أو الأحداث، وهي أخبار مبالغ فيها ومكررة.

أما الأخبار المغرضة في تلك التي تنطوي على بعض الحقيقة ولكنها تذاع وتنشر بشيء من التحريف أو الخوف بما يجعلها في حكم الأخبار الكاذبة، فالخبر المحرف الذي فيه لي للحقيقة مع وجه يشوهها هو خبر مغرض[130]. وأما إثارة الفزع فهي استيلاء الهلع والرعب بين الناس، فلا يشعرون بالأمان في سيرهم وغدوهم وتجولهم وإقامتهم، ويتوجسون الخوف والفزع من احتمال حدوث ما يعكر صفو حياتهم ويهدد العيش في المجتمع.

وأما تكدير السلم العام، فالسلم العام هو الإحساس بالأمن والطمأنينة ونفي الخوف عن المواطنين والاستمتاع بحياتهم بشكل طبيعي، فأي خبر أو بيان أو إشاعة كاذبة أو إشارة مغرضة أو مثيرة، تستهدف منع الناس من إداء أعمالهم أو كفهم عن ممارسة حياتهم الطبيعية المشروعة، يمثل تكديرًا للسلم العام.

ثانيًا: النتيجة الاجرامية:

بين المشرع البحريني النتيجة الإجرامية التي يسعى الجاني إلى تحقيقها عبر إذاعة الأخبار أو البيانات أو الإشاعات الكاذبة أو المغرضة أو إذاعة دعاية مثيرة عبر مواقع التواصل الاجتماعي، وهذه النتيجة قد تتمثل في أن يمون من شأن سلوك الجاني إلحاق الضرر بالاستعدادات الحربية للدفاع عن دولة البحرين أو بالعمليات

---

129 د. عبدالحميد الشواربي، الجرائم التعبيرية، جرائم الصحافة والنشر، دار الكتب والدراسات العربية، الاسكندرية، 2018، ص149.

130 د. عبدالحميد الشواربي، المرجع السابق، ص194.

الحربية للقوات المسلحة أو إثارة الفزع بين الناس أو إضعاف الجلد في الأمة وتثبيط عزيمتها، أو إضعاف الثقة المالية بالدولة أو النيل من هيبتها أو اعتبارها، أو الإضرار بالمصالح القومية، أو من الممكن أن تحدث ضررًا بالأمن الوطني أو بالنظام العام أو بالصحة العامة متى ترتب على ذلك حدوث الضرر، أو تكدير السلم العام أو الحاق الضرر بمصلحة عامة.

ثالثًا: الشروع في الجريمة:

الشروع في هذه الجريمة كصورة من صور الركن المادي متصور، كما لو قام الجاني بمحاولة إذاعة إشاعة أو خبر كاذب ولكن الجهاز الذي أستخدمه لم يسعفه في الإذاعة والنشر، أو تم ضبط الجاني عندما بدأ بالإذاعة أو النشر للبيان أو الخبر الكاذب أو الإشاعة الكاذبة أو المغرضة. فأغلب صور هذه الجريمة من جرائم الضرر، أي الجرائم المادية ذات النتيجة التي يتحقق فيها الشروع المعاقب عليه في الجنايات وأما الجنح فلا يعاقب المشرع البحريني على الشروع فيها[131].

الفرع الثالث: الركن المعنوي:

الركن المعنوي لجريمة إذاعة الشائعة والأخبار الكاذبة يتمثل بالقصد الجنائي، وهو توجيه الفاعل إرادته نحو اقتراف سلوك إجرامي إيجاني أو سلبي وهو يدرك تمامًا أنه ينتهك به النصوص التجريمية[132].

فالقصد الجنائي لجريمة إذاعة الشائعة والأخبار الكاذبة هو علم الجاني بعناصر الجريمة كما حددها النموذج القانوني للجريمة واتجاه إرادته إلى تحقيق هذه العناصر أو قبوله لها[133].

وفي جريمة إذاعة الشائعة والأخبار الكاذبة تتجه إرادة الفاعل إلى القيام بإذاعة الشائعة والأخبار الكاذبة أو ترويجها عبر وسائل التواصل الاجتماعي وهو يعلم بأن فعله هذا مجرم قانونًا وأنه سوف تترتب عليه إلحاق الضرر بالأمن الوطني أو بالقوات المسلحة أو خطط الدفاع والعمليات العسكرية أو الإضرار بالاقتصاد الوطني أو بالصحة العامة أو تعريضها للخطر، وإرادة تلك النتائج ألمترتبة على ذلك أوقبوله لها.

---

[131] **تنص المادة (38) من قانون العقوبات البحريني على أنه " لا يعاقب على الشروع في الجنح إلا في الحالات التي ينص عليها القانون".**

[132] **د.عبد الوهاب حومد، الوسيط في شرح قانون الجزاء الكويتي، منشورات جامعة الكويت، 1987، ص92.**

[133] **محمد منصور البابا، تجريم الشائعة في التشريع الأردني – دراسة مقارنة، رسالة ماجستير مقدمة إلى كلية الحقوق بجامعة الشرق الأوسط، الأردن، 2020، ص78.**

_ تاريخ الولوج 2021/7/6.https://meu.edu.jo/libraryTheses/A.pdf

فالعلم يجب أن ينصرف إلى طبيعة فعل الشائعة ونتيجته الاجرامية وإلى موضوع الحق المعتدى عليه والظروف الداخلة في تكوين الجريمة وزمان إرتكابها، وضرورة إقتران العلم بالإرادة.

المبحث الثالث: عقوبة جريمة إذاعة الشائعة والأخبار الكاذبة

تمهيد وتقسيم: سوف نتناول في هذا المبحث العقوبات المقررة لجريمة إذاعة وترويج الشائعات والأخبار الكاذبة، وهذه العقوبات إما أن تكون عقوبات أصلية وإما أن تكون عقوبات فرعية، وهذا يقتضي منا تقسيم هذا المبحث إلى مطلبين، أولهما: العقوبات الأصلية، وثانيهما: العقوبات الفرعية.

المطلب الأول: العقوبة الأصلية المقررة لجريمة إذاعة الشائعة والأخبار الكاذبة:

تعرف العقوبة بأنها "جزاء مقرر بنص القانون ويوقعه القاضي على من تثبت مسؤوليته عن فعل يعد جريمة ليصيب به المتهم في شخصه أو ماله أو شرفه"[134]، وقد ربط المشرع البحريني بشكل دقيق نوع العقوبة ومقدارها بتكييف الجريمة القانوني الذي يستند إلى طبيعة المصلحة أو الحق الذي تستهدف الجريمة الحاق الضرر به أو تعريضه للخطر، وسوف نتناول العقوبات الأصلية المقررة لجريمة إذاعة الشائعات والأخبار الكاذبة في التشريع الجنائي البحريني تباعاً:

اولًا: عقوبة الحبس والغرامة أو أحدهما: لقد قرر المشرع البحريني عقوبة الحبس مدة لا تقل عن ثلاثة أشهر والغرامة التي لا تقل عن مائة دينار أو بإحدى العقوبتين في المادة (134) من قانون العقوبات، كعقوبة مقررة لجريمة قيام المواطن في الخارج بتعمد إذاعة أخبار أو بيانات أو إشاعات كاذبة أو مغرضة حول الأوضاع الداخلية للدولة إذا كان من شأن ذلك إضعاف الثقة المالية بالدولة أو النيل من هيبتها أو اعتبارها، أو باشر بأية طريقة نشاطًا من شأنه الإضرار بالمصالح القومية، وهنا يتضح بأن الجريمة في صورتها البسيطة جنحة . فإذا وقعت الجريمة في زمن الحرب تشدد العقوبة إلى السجن مدة لا تزيد على عشر سنوات، وهنا تتحول الجريمة إلى جناية إذا توافر ظرف التشديد وهو وقوع الجريمة في زمن الحرب.

ونلاحظ أن المشرع قرر العقوبة المذكورة إذا ارتكب المتهم فعلاً من أفعال إذاعة أخبار أو بيانات أو إشاعات كاذبة أو مغرضة على ما هو موصوف بالنص دون أن ينتظر تحقق النتائج الضارة، حيث يكفي حصول الفعل المتجه بحسب طبيعته وقصد الفاعل إلى إحداث نتيجة ضارة، وهو بهذا يساوى بين وقوع نتيجة ضارة

---

[134] د. محمد زكي أبو عامر، مبادئ علم الاجرام وعلم العقاب، الدار الجامعة للنشر، الاسكندرية،1992، ص435.

وبين عدم وقوعها، مما يعني أن جرائم إذاعة الأخبار أو البيانات أو الإشاعات الكاذبة هي من جرائم الخطر، لأن المشرع استخدم عبارة "..... من شأنه إضعاف..... من شأنه الإضرار..".

كما قرر المشرع البحريني في المادة (168) من قانون العقوبات، عقوبة الحبس مدة لا تزيد على سنتين وبالغرامة التي لا تتجاوز مائتي دينار أو بإحدى العقوبتين لمن يرتكب جريمة تعمد إذاعة أخبار كاذبة مع علمه بأنها من الممكن أن تحدث ضررًا بالأمن الوطني أو بالنظام العام أو بالصحة العامة متى ترتب على ذلك حدوث الضرر. وقد اشترط المشرع في الأخبار الكاذبة المتعلقة بإحداث الضرر بالأمن الوطني أن تكون تحريضًا على العنف أو من شأنها أن تحرض عليه، وأن يكون بين تلك الأخبار الكاذبة وبين حدوث العنف أو احتمالية حدوثه رابط مباشر.

وحسنًا فعل المشرع البحريني حيث جعل العقاب شاملاً الجريمة إذا كان من شأنها أن تحدث ضررًا بالصحة العامة، إذ كثرت الشائعات والأخبار الكاذبة التي أنتشرت مؤخرًا في وسائل التواصل الاجتماعي عن اللقاحات الخاصة بجائحة كورونا، مما ترتب عليها إثارة الفزع والخوف في أوساط الناس وأدت إلى إلحاق أضرار بالغة بالاقتصاد الوطني والصحة العامة وعرقلة الجهود التي تقوم بها السلطات المختصة بمكافحة الجائحة، حيث أدت تلك الشائعات إلى عزوف الناس وخوفهم من تلقي اللقاحات التي وفرتها الدولة لمواجهة فيروس كورونا، وهو ما يؤدي إلى إزدياد الإصابات بين المواطنين والمقيمين ومن ثم زيادة الأعباء المالية على كاهل الدولة لمواجهة تلك الزيادات من توفير العلاجات وتعطل المصابين والمخالطين عن العمل خلال تلقي العلاج أو الحجر وكذلك إضطرار السلطات إلى إغلاق المحلات التجارية وكذلك تحمل الخزينة العامة للدولة دفع مساعدات مالية كبيرة للكثير من الشركات الخاصة وأصحاب المشروعات الصغيرة التي تأثرت بالجائحة، وهو ما يلحق خسائر كبيرة بالاقتصاد الوطني، فضلاً عن الوفيات وهي بلا شك خسائر جسيمة.

الأعذار المخففة للعقاب والإعفاء منه: وإذا تعدد المساهمون في الجريمة المصوص عليها في المادة (134) من قانون العقوبات، فإنه طبقًا للمادة (144) من القانون ذاته إذا بادر أحدهم إلى إبلاغ السلطات القضائية أو الإدارية عن الجريمة قبل البدء في التحقيق، فإن العقوبة تخفف عنه بإعتبار الابلاغ عذر قانوني مخفف، كما أجاز المشرع للقاضي في هذه الحالة إعفاء الجاني الذي بادر بالابلاغ من العقوبة إذا رأى محلاً لذلك، فالامر في هذه الحالة الأخيرة متروك أمر تقرير الإعفاء لسلطة القاضي التقديرية، وهو ما يعرف بالعفو القضائي.

وتسري الأحكام ذاتها بالنسبة للمساهم الذي يمكن السلطات أثناء التحقيق من القبض على مرتكبي الجريمة الآخرين.

إذا تعدد المساهمون في إقتراف جريمة تعمد إذاعة أخبار كاذبة فإنه طبقًا للمادة (177) من القانون ذاته إذا بادر أحد المساهمين فيها بإبلاغ السلطات القضائية أو الإدارية عن وقوع الجريمة قبل البدء في التحقيق الابتدائي، فإن ذلك الإبلاغ يعدُ عذرًا قانونيًا مخففًا للعقوبة عنه. كما يجوز للقاضي وفقًا لسلطته التقديرية إعفاء المبلغ من العقوبة إذا رأى محلاً لذلك. وتسري الأحكام السابقة بالنسبة للجاني الذي يمكن السلطات أثناء التحقيق من القبض على المساهمين الآخرين في ارتكاب الجريمة.

ثانيًا: عقوبة السجن: قرر المشرع البحريني عقوبة السجن المؤقت مدة لا تزيد على عشر سنوات في المادة (133) من قانون العقوبات، كجزاء مقرر لجريمة قيام الجاني بتعمد إذاعة أخبار أو بيانات أو إشاعات كاذبة أو مغرضة أو عمد إلى دعاية مثيرة في زمن الحرب، وكان من شأن الجريمة إلحاق الضرر بالاستعدادات الحربية للدفاع عن مملكة البحرين أو بالعمليات الحربية لقواتها المسلحة أو أثار الفزع بين الناس أو إضعاف معنويات الأمة. وتشدد العقوبة إذا ارتكبت الجريمة نتيجة للتخابر مع دولة أجنبية إلى السجن من ثلاث سنوات إلى خمس عشرة سنة. وتشدد العقوبة إلى السجن المؤبد إذا ارتكبت الجريمة نتيجة للتخابر مع دولة معادية للمملكة.

وهنا نلاحظ أن الجريمة في كل أوصافها البسيطة والمشددة تعد جناية، والمشرع أعتبر هذه الجريمة جريمة خطر، حيث أستخدم عبارة "....... وكان من شأن الجريمة إلحاق الضرر ....."، مما يعني أن المشرع لا ينتظر وقوع النتيجة الضارة للعقاب بل يعاقب الجاني ولو لم تحصل النتيجة الضارة ويكتفي بإمكانية حدوثها، أي أنه ساوى في العقوبة بين تحقق النتيجة الضارة وبين عدم تحققها طالما أن قصد الجاني كان متجهًا ابتداء إلى تحقيقها.

الأعذار المخففة للعقاب والإعفاء منه: وفقًا للمادة (144) من القانون ذاته إذا تعدد المساهمين في الجريمة المنصوص عليها في المادة (133) من قانون العقوبات وبادر أحدهم إلى إبلاغ السلطات القضائية أو الإدارية عن الجريمة قبل البدء في التحقيق، فإن العقوبة تخفف عنه بإعتبار الابلاغ عذر قانوني مخفف، كما أجاز المشرع للقاضي في هذه الحالة إعفاء الجاني الذي بادر بالابلاغ من العقوبة إذا رأى محلاً لذلك، فالامر في هذه الحالة الأخيرة متروك أمر تقرير الإعفاء لسلطة القاضي التقديرية، وهو ما يعرف بالعفو القضائي.

وتسري الأحكام ذاتها بالنسبة للمساهم الذي يمكن السلطات أثناء التحقيق من القبض على مرتكبي الجريمة الآخرين.

ثالثًا: عقوبة الإعدام: أجازت المادة (142) من القانون ذاته للمحكمة الحكم بالإعدام عن هذه الجريمة متى كان قصد الجاني منها إعانة العدو أو الإضرار بالعمليات الحربية للقوات المسلحة وكان من شأن الجريمة تحقيق الغرض المذكور، حيث نصت هذه المادة على أنه: " يجوز الحكم بالإعدام في الجنايات الواردة في هذا الفصل[135] متى قصد الجاني منها إعانة العدو أو الإضرار بالعمليات الحربية للقوات المسلحة وكان من شأنها تحقيق الغرض المذكور".

وفي حالة تعدد المساهمين في اقتراف الجريمة فإنه وفقًا للمادة (144) من قانون العقوبات إذا بادر أحدهم إلى إبلاغ السلطات القضائية أو الإدارية عن الجريمة قبل البدء في التحقيق، فإن العقوبة تخفف عنه بإعتبار الابلاغ عذر قانوني مخفف، كما أجاز المشرع للقاضي في هذه الحالة إعفاء الجاني الذي بادر بالابلاغ من العقوبة إذا رأى محلًا لذلك، فالامر في هذه الحالة الأخيرة متروك أمر تقرير الإعفاء لسلطة القاضي التقديرية.

رابعًا: عقوبة الغرامة: قرر المشرع البحريني في المادة (134) من قانون العقوبات عقوبة الغرامة التي لا تقل عن مائة دينار على كل مواطن أذاع عمدًا في الخارج أخبار أو بيانات أو إشاعات كاذبة أو مغرضة حول الأوضاع الداخلية للدولة إذا كان من شأنها إضعاف الثقة المالية بالدولة أو النيل من هيبتها أو اعتبارها، أو باشر بأية طريقة كانت نشاطًا من شأنه الإضرار بالمصالح القومية. كما فرض عقوبة الغرامة التي لا تتجاوز مائتي دينار على من أذاع عمدًا أخبار كاذبة مع علمه بأنها من الممكن أن تحدث ضررًا بالأمن الوطني أو بالنظام العام أو بالصحة العامة، متى ترتب على ذلك حدوث الضرر.

كما عاقبت المادة (70) من قانون الصحافة جريمة نشر الأخبار الكاذبة بالعقوبة المنصوص عليها في المادة (69) منه، وهي عقوبة الغرامة التي لا تزيد على الفي دينار.

المطلب الثاني: العقوبات الفرعية المقررة لجريمة إذاعة الشائعات والأخبار الكاذبة:

من العقوبات الفرعية التي قررها المشرع البحريني لجريمة إذاعة الشائعات والأخبار الكاذبة ، عقوبة المصادرة وعقوبة الحرمان من بعض الحقوق والمزايا وعقوبة الحجر القانوني وعقوبة العزل من الوظيفة أو الخدمة العامة.

---

[135] **هذا الفصل خاص بجرائم أمن الدولة الخارجي.**

اولاً: عقوبة المصادرة: نص المشرع البحريني في قانون العقوبات على أنه:" يجوز للقاضي إذا حكم بعقوبة لجريمة أن يحكم بمصادرة الأشياء المضبوطة التي تحصلت منها أو التي استعملت فيها أو كان من شأنها أن تستعمل فيها.

ويحكم القاضي بمصادرة الأشياء المذكورة مما يعد صنعها أو حيازتها أو إحرازها أو استعمالها أو التعامل فيها جريمة ولو لم تكن مملوكة للمتهم أو لم يكن قد صدر في الدعوى حكم بالإدانة.

وعلى القاضي أن يحكم بمصادرة الأشياء التي جعلت أجرا لارتكاب الجريمة.

وهذا كله بدون إخلال بالحقوق العينية التي للغير الحسن النية"[136].

وعقوبة المصادرة هنا مقررة سواء كانت الجريمة جناية أو جنحة، ولكن لا يمكن الحكم بها إلا إذا كان قد سبقها إجراء الضبط والتحريز، لأن الحكم بمصادرة الأشياء التي تحصلت من جريمة بث الشائعات الكاذبة أو استعملت فيها أو كانت معدة للاستعمال فيها لا يمكن مالم تكن تلك الأشياء قد ضبطت، فالنص جاء بصيغة " ... الأشياء الضبوطة...." وهذا أمر منطقي. فمثلاً لو تم إذاعة أخبار أو بيانات كاذبة عبر وسائل التواصل الاجتماعي وكان ذلك نظير مقابل مادي مودع في البنك مثلاً يجوز الحكم بمصادرته، فالمشرع أجاز مصادرة الأشياء التي جعلت أجرًا لارتكاب الجريمة، كما يحكم بأجهزة الحاسب الآلي أو الهواتف النقالة التي استعملت في ارتكاب الجريمة.

ثانيًا: عقوبة الحرمان من الحقوق والمزايا المنصوص عليها في المادة (53)[137]: قرر المشرع البحريني عقوبة الحرمان من الحقوق والمزايا في قانون العقوبات بقوله:" الحكم بالسجن يستتبع الحرمان من كل الحقوق والمزايا المنصوص عليها في المادة 53 وذلك من يوم الحكم حتى نهاية تنفيذ العقوبة أو انقضائها بأي

---

[136] المادة (64) من قانون العقوبات البحريني.

[137] تنص المادة (53) من قانون العقوبات البحريني :" التجريد المدني هو حرمان المحكوم عليه من كل أو بعض الحقوق والمزايا الآتية:

1- الحق في تولي الوظائف والخدمات العامة.
2- الحق في أن يكون ناخبا أو منتخبا في المجالس العامة.
3- الحق في أن يكون ناخبا أو منتخبا في الهيئات المهنية والنقابية.
4- الصلاحية لأن يكون عضوًا في مجلس إدارة شركة مساهمة أو مديرا لها.
5- الصلاحية لأن يكون خبيرا.
6- الصلاحية لأن يكون مديرا أو ناشرا لإحدى الصحف.
7- الصلاحية لتولي إدارة مدرسة أو معهد.
8- حمل أوسمة وطنية أو أجنبية".

سبب أخر...........". ويلاحظ أن عقوبة الحرمان من الحقوق المقررة في النص السابق هي عقوبة فرعية تبعية وجوبية في الجنايات المعاقب عليها بالسجن.

أما المادة (61) من قانون العقوبات فقد قررت عقوبة الحرمان من الحقوق والمزايا كعقوبة فرعية تكميلة في الجنايات بقولها :" للقاضي عند الحكم بالإدانة في جناية أن تأمر بحرمان المحكوم عليه من حق أو مزية أو أكثر مما نص عليه في المادة 53 وذلك لمدة لا تقل عن سنة ولا تزيد على عشر سنوات تبدأ من نهاية تنفيذ العقوبة أو انقضائها لأي سبب أخر.

وإذا كانت العقوبة المحكوم بها هي الحبس امتد الحرمان المقضي به إلى فترة وجود المحكوم عليه بالسجن".

من النصين السابق نجد أن عقوبة الحرمان من الحقوق والمزايا عقوبة فرعية تكميلية جوازية في الجنايات حتى ولو حكم فيها القاضي بعقوبة الحبس بدلًا عن السجن عند توافر ظرف قضائي أو عذر قانوني مخفف، ولكن مدة الحرمان تختلف ففي حالة الحكم بالسجن تكون مدة الحرمان لا تقل عن سنة ولا تزيد على عشر سنوات تبدأ من نهاية تنفيذ عقوبة السجن أو انقضائها لأي سبب، بينما إذا كان حكم الإدانة في الجناية كان عقوبة الحبس أمتد الحرمان المقضي به إلى فترة وجود المحكوم عليه بالسجن فقط،. ولذا يحكم بعقوبة الحرمان من الحقوق والمزايا إذا ارتكبت جناية أو جنحة إذاعة الشائعة والأخبار الكاذبة عبر وسائل التواصل الاجتماعي كعقوبة فرعية تبعية.

ثالثًا: عقوبة الحجر القانوني: لقد قرر المشرع البحريني عقوبة الحجر القانوني كعقوبة فرعية تبعية للعقوبة الأصلية في الجرائم الصادر فيها حكم بالإعدام أو السجن المؤبد أو المؤقت، لإذ نصت المادة (58) من قانون العقوبات على أنه:" كل حكم صادر بالإعدام يستتبع بقوة القانون بطلان كل أعمال التصرف والإدارة التي تصدر عن المحكوم عليه عدا الوصية.

ويعين على أموال المحكوم عليه قيم تتبع في إجراءات تعيينه وتحديد سلطاته الأحكام المعمول بها في شأن القوامة على المحجور عليهم".

كما نصت المادة (59) من قانون العقوبات البحريني على أنه :" الحكم بالسجن يستتبع الحرمان من كل الحقوق والمزايا ....

ويقع باطلا كل عمل من أعمال التصرف أو الإدارة إذا صدر من المحكوم عليه بالسجن خلال مدة سجنه.

ويعين على أمواله قيم تتبع في إجراءات تعيينه وتحديد سلطاته الأحكام المعمول بها في شأن القوامة على المحجور عليهم".

ومن خلال النصين السابقين نجد أن عقوبة الحجر القانوني تقع بقوة القانون في الجنايات المعاقب عليها بالإعدام أو بالسجن المؤبد أو المؤقت، وحيث أن جريمة إذاعة الشائعات والأخبار الكاذبة كما رأينا قد يحكم فيها بالسجن المؤقت أو المؤبد وفقًا للمادة (333) عقوبات ويجوز الحكم فيها بالإعدام وفقًا للمادة (142) من قانون العقوبات، فإن الحكم بالإعدام أو بالسجن في هذه الجريمة يستتبع بقوة القانون فرض عقوبة الحجر القانوني عليه.

رابعًا: عقوبة العزل من الوظيفة أو الخدمة العامة: هذه العقوبة قررها المشرع البحريني كعقوبة فرعية تبعية في المادة (60) من قانون العقوبات التي تنص على أنه :

" إذا كان المحكوم عليه موظفا عاما أو مكلفا بخدمة ترتب على حرمانه من الحق في تولي الوظائف أو الخدمات العامة عزله منها". وفقا لهذا النص إذا كان مقترف جريمة إذاعة الشائعة أو الأخبار الكاذبة موظف عام أو مكلف بخدمة عامة وحكم بحرمانه من تولي الوظائف أو الخدمات العامة، فإن ذلك الحكم يستتبع بقوة القانون عزله من الوظيفة.

وهذه العقوبة تفرض على الموظف بقوة القانون على الموظف العام سواء كانت الجريمة جنحة أم جناية.

الخاتمة

بعد أن انتهينا من دراسة موضوع المسؤولية الجنائية الناشئة عن جريمة إذاعة الشائعة والأخبار الكاذبة عبر وسائل التواصل الاجتماعي، توصلنا إلى جملة من النتائج والتوصيات وكما يلي:

اولًا: النتائج:

- خلصت الدراسة إلى أن وسائل التواصل الاجتماعي المختلفة تُعدُ من أخطر وسائل إذاعة ونشر الشائعة أو الاخبار الكاذبة في الوقت الراهن والمستقبل المنظور.

- خلصت الدراسة إلى أن نشر الشائعة أو الأخبار الكاذبة عبر مواقع التواصل الاجتماعي تنهض بها المسؤولية الجنائية.

- خلصت الدراسة إلى أن الشائعة وإن كانت نشاط يمارس منذ القدم إلا أننا لم نجد لها تعريفًا لدى فقهاء القانون القدماء، إذ من خلال الكتب الفقهية التي أطلعنا عليها لم نلق فيها تعريف الشائعة، وإن كانت كتب علم النفس الاجتماعي أو الحرب النفسية والرأي العام قد عرفت الشائعة، ولذا يمكننا عد الشائعة لدى فقهاء القانون من المصطلحات الحديثة وخاصة حال ارتكابها عبر وسائل التواصل الاجتماعي في هذا العصر. وقد عرفنا الشائعة الإلكترونية بأنها، إذاعة وترويج الأخبار الكاذبة أو المضللة عن دولة أو شخص أو حدث ما بأي وسيلة الكترونية بهدف التأثير في جمهور المتلقين والحاق الضرر بأمن الدولة أو جيشها أو اقتصادها أو نظامها الصحي.

- توصلت الدراسة إلى أن جريمة إذاعة الشائعة والأخبار الكاذبة بأنها قد تكون جريمة ضرر وقد تكون جريمة خطر، إذ توصلنا إلى أن المشرع البحريني يساوي في العقوبة سواء تخلف عن الجريمة ضرر فعلي بالمصلحة المحمية أو لم يتخلف عنها ذلك الضرر ويكفي للعقاب مجرد تعريض تلك المصلحة للخطر.

- توصلت الدراسة إلى أن جريمة إذاعة الشائعة أو الأخبار الكاذبة تعد من الجرائم العمدية التي يقوم ركنها المعنوي على القصد الجنائي ولا تقوم الجريمة على الخطأ غير العمدي.

- توصلت الدراسة إلى أن المشرع البحريني قد جرم إذاعة الشائعة أو الأخبار الكاذبة التي تقترف عبر وسائل التواصل الاجتماعي وذلك في المادة (23) من قانون جرائم تقنية المعلومات التي أحالت إلى الجرائم المنصوص عليها في القوانين الأخرى في كل ما لم يرد به نص في هذا القانون إذا ارتكبت بوسيلة تقنية معلومات ويعاقب مرتكبها بالعقوبة المقررة للجريمة، وبهذا النص تحقق مبدأ شرعية الجرائم الالكترونية.

- خلصت الدراسة أن جريمة إذاعة الشائعة قد تكون جناية يعاقب فاعلها بالسجن المؤقت أو المؤبد، ويجوز أن تصل العقوبة إلى الإعدام وفقا المادة (142) عقوبات، وقد تكون جنحة يعاقب عليها بالحبس والغرامة معا أو بإحدى العقوبتين.

ثانيًا: التوصيات:

1- نوصي المشرع البحريني بإضافة نصوص إلى قانون العقوبات تتضمن تجريم إذاعة الشائعة أو البيانات أو الأخبار الكاذبة إذا ارتكبت الجريمة الكترونيًا عبر وسائل التواصل الاجتماعي أو غيرها من وسائل تقنية الاتصالات والمعلومات.

2- نوصي المشرع البحريني تجريم إذاعة الشائعة أو البيانات أو الأخبار الكاذبة عبر وسائل التواصل الاجتماعي إذا كان من شأنها إضعاف الثقة بالنظام الالكتروني للدولة.

3- نوصي المشرع البحريني تجريم إذاعة أو نشر شائعة أو بيانات أو أخبار كاذبة عبر وسائل التواصل الاجتماعي من شأنها إضعاف الثقة بالنظام المالي الالكتروني أو الأوراق المالية الالكترونية وما في حكمها أو الحاق الضرر بالاقتصاد الوطني أو زعزعة الثقة بالدولة.

4- نوصي المشرع البحريني تجريم إذاعة أو نشر شائعة أو بيانات أو أخبار كاذبة أو مضللة عبر وسائل التواصل الاجتماعي إذا كان من شأنها إثارة النعرات الطائفية أو المذهبية أو الكراهية أو تكدير الأمن والنظام العام أو الإساءة للدولة أو رموزها.

5- نوصي بقيام حملة إعلامية مكثفة للتوعية بمخاطر إذاعة الشائعة أو الأخبار الكاذبة والآثار المترتبة على ذلك على مستوى الفرد والمجتمع وبيان المسؤولية القانونية الناشئة عنها.

6- نوصي المشرع البحريني بتجريم كل نشر لأخبار أو صور تمس الحياة الخاصة للأفراد أو التقاط صور أو مقاطع فيديو لهم دون رضاهم أو نقل سجلات المحادثات الخاصة إلى العلن أو الفضاء العام دون رضا المشاركين فيها أو نقل أو تسجيل محادثة في مكان خاص أو القيام بإعداد أو نقل محادثة صورة أو فيلم لشخص في وضع خاص أو غير لائق وإن كان ما تم إعداده أو نقله مزيفًا وغير حقيقي.

قائمة المصادر

اولًا: المراجع باللغة العربية:

أ- الكتب والبحوث والمعاجم:

1- جمال الدين محمد بن مكرم ابن منظور، لسان العرب، دار صادر، بيروت، ج 10، 1982.
2- د. دنيا عبدالعزيز فهمي، الحماية الجنائية من إساءة استخدام مواقع التواصل الاجتماعي- دراسة مقارنة، دار النهضة العربية، 2018.
3- د. عباس الحسني، علم النفس العسكري، ج1، مطبعة الرشاد، بغداد، 1968.
4- د. عبدالحميد الشواربي، الجرائم التعبيرية، جرائم الصحافة والنشر، دار الكتب والدراسات العربية، الاسكندرية، 2018.
5- د.عبد الوهاب حومد، الوسيط في شرح قانون الجزاء الكويتي، منشورات جامعة الكويت، 1987.
6- د.علي حسن الشرفي، أحكام الشائعات في القانون العقابي المقارن، بحث مقدم إلى مؤتمر أساليب مواجهة الشائعات، أكاديمية نايف للعلوم الأمنية – الرياض- 2001.
7- د. فخري عبدالرزاق الحديثي، شرح قانون العقوبات – القسم العام، مكتبة السنهوري، بيروت، لبنان، 2018.
8- د. محمد روا قلعه جي ود. حامد صادق قنيبي، معجم لغة الفقهاء، دار النفائس للطباعة والنشر بيروت، لبنان، ط1، 1988.
9- مجمع اللغة العربية، مصر، المعجم الوسيط، مكتبة الشروق الدولية ج1،ط4، باب السين،2004.
10- د. محمد أبو زهرة، الجريمة والعقوبة في الفقه الإسلامي، دار الفكر العربي، القاهرة، بدون.
11- د. محمد زكي أبو عامر، مبادئ علم الاجرام وعلم العقاب، الدار الجامعة للنشر، الاسكندرية،1992.
12- محمد مرتضى الحسيني الزبيدي، تاج العروس من جواهر القاموس، تحقيق مجموعة من المحققين، دار الهداية، باب العين المهملة، مادة شيع، (5356/1).
13- د.محمد مصطفى القللي، في المسؤولية الجنائية، مطبعة عبدالله وهبة، مصر، 1945.
14- د. محمود نجيب حسني، شرح قانون العقوبات – القسم العام اللبناني، المجلد الأول، مشورات الحلبي الحقوقية، ط3، بدون سنة نشر.
15- د. محمود نجيب حسني، شرح قانون العقوبات – القسم العام، دار النهضة العربية، القاهرة، 1989.

ب- مواقع الكترونية:

1- تسنيم معابرة ، أهم مواقع التواصل الاجتماعي، منشمر على موقع الويب .
2- https://mawdoo3.com/

3- د. سلمان بن عبدالله بن حمود أبا الخيل، مقومات المواطنة الصالحة، نص محاضرة القاها في جامع الامام تركي بن عبدالله بالرياض.

http://islamancient.com/ressources/docs/366.pdf.

4- محمد منصور البابا، تجريم الشائعة في التشريع الأردني – دراسة مقارنة، رسالة ماجستير مقدمة إلى كلية الحقوق بجامعة الشرق الأوسط، الأردن، 2020، ص78. منشور على موقع.

https://meu.edu.jo/

ثانيًا: المراجع باللغة الانجليزية:

[1] Rudat,A. Twitter Spreads Rumors: Influencing Factors on Twitter's Role in Rumor Spread Among University Students, PhD Thesis, Tubingen: Tubingen. 2015.

ثالثًا: القوانين:

1- قانون العقوبات البحريني رقم (15) لسنة 1976.

2- قانون جرائم تقنية المعلومات رقم (60) لسنة 2014.

3- المرسوم بقانون رقم (5) لسنة2012 نشأن مكافحة جرائم تقنية المعلومات الإماراتي.

الجرائم الرقمية بين: الرقابة المعالجة

الدكتور مصطفى الفوركي
مدير مجلة القانون والأعمال الدولية (المغرب)

الجريمة الإلكترونية هي فعل يتسبب بضرر جسيم للأفراد أو الجماعات والمؤسسات، بهدف ابتزاز الضحية وتشويه سمعتها من أجل تحقيق مكاسب مادية أو خدمة أهداف سياسية باستخدام الحاسوب ووسائل الإتصال الحديثة مثل الإنترنت.

فتكون الجرائم المعلوماتية بهدف سرقة معلومات واستخدامها من أجل التسبب بأذى نفسي ومادي جسيم للضحية، أو إفشاء أسرار أمنية هامة تخص مؤسسات هامة بالدولة أو بيانات وحسابات خاصة بالبنوك والأشخاص،

تتشابه الجريمة الإلكترونية مع الجريمة العادية في عناصرها من حيث وجود الجاني والضحية وفعل الجريمة،

ولكن تختلف عن الجريمة العادية باختلاف البيئات والوسائل المستخدمة، فالجريمة الإلكترونية يمكن أن تتم دون وجود الشخص مرتكب الجريمة في مكان الحدث، كما أن الوسيلة المستخدمة هي التكنولوجيا الحديثة ووسائل الإتصال الحديثة والشبكات المعلوماتية.

إضافة إلى تنامي ظاهرة الغزو السايبراني وما أفرزته من مظاهر التثاقف والإنكشافية الإعلامية التي جعلت الفضاء الداخلي منفتحا على جميع المؤثرات الخارجية، مع عدم القدرة على التحكم في سعة وحجم التدفقات المعرفية وقوتها التأثيرية على عقول وسلوك المتلقين بسبب الترابط الشبكي المعقد بين الأشخاص، ولهذا أصبحت الأحداث الواقعة في أقاصي الأرض تلقي بظلالها وآثارها على الجانب الآخر، فظهرت التنظيمات والترابطات الشبكية العابرة للحدود، وهو ما شكل تحديا كبيرا على المؤسسات الأمنية والتعليمية والإجتماعية والأمن المجتمعي والفكري عموما.

فكما تعلمون ان التطور التقني والرقمي الحديث أنتج تطبيقات ومظاهر جديدة اجتاحت مختلف مناحي الحياة، وبرزت إزاءها أشكال متنوعة لجرائم مرتبطة بسوء استخدام تكنولوجيا المعلومات والاتصالات ومنها :

يمكن تقسيم أنواع الجرائم الالكترونية الى جرائم تسبب الأذى للفرد

ثانيا: جرائم تسبب الأذى للمؤسسات

ثالثا: جرائم الأموال.

رابعا: الجرائم التي تستهدف أمن الدولة.

اولا: جرائم تسبب الأذى للأفراد.

ومن خلالها يتم استهداف فئة من الأفراد أو فرد بعينه من أجل الحصول على معلومات هامة تخص حساباته سواء البنكية أو على الإنترنت، وتتمثل هذه الجرائم في:

- **انتحال الشخصية :** وفيها يستدرج المجرم الضحية ويستخلص منها المعلومات بطرق غير مباشرة، ويستهدف فيها معلومات خاصة من أجل الإستفادة منها واستغلالها لتحقيق مكاسب مادية أو التشهير بسمعة أشاص بعينهم وقلب الوسط رأساً على عقب، وإفساد العلاقات سواء الإجتماعية أو علاقات العمل.
- **تهديد الأفراد:** يصل المجرم من خلال القرصنة وسرقة المعلومات إلى معلومات شخصية وخاصة جداً بالنسبة للضحية، ثم يقوم بابتزازه من أجل كسب الأموال وتحريضه للقيام بأفعال غير مشروعة قد يصاب فيها بأذى.
- **تشويه السمعة:** يقوم المجرم باستخدام المعلومات المسروقة وإضافة بعض المعلومات المغلوطة، ثم يقوم بارسالها عبر الوسائط الإجتماعية أو عبر البريد الإلكتروني للعديد من الأفراد بغرض تشويه سمعة الضحية وتدميرهم نفسياً.
- **تحريض على أعمال غير مشروعة:** يقوم المجرم باستخدام المعلومات المسروقة عن أفراد بعينهم واستغلالها في ابتزاز الضحايا بالقيام بأعمال غير مشروعة تتعلق بالدعارة وتجارة المخدرات وغسيل الأموال والعديد من الجرائم الإلكترونية الأخرى.

ثانيا: جرائم تسبب الأذى للمؤسسات.

اختراق الأنظمة:

- وتتسبب الجرائم الإلكترونية بخسائر كبيرة للمؤسسات والشركات المتمثلة في الخسائر المادية والخسائر في النظم، بحيث يقوم المجرم باختراق أنظمة الشبكات الخاصة بالمؤسسات والشركات والحصول على

معلومات قيمة وخاصة بأنظمة الشركات، ومن ثم يقوم باستخدام المعلومات من أجل خدمة مصالحه الشخصية والتي تتمثل في سرقة الأموال وتدمير أنظمة الشركة الداعمة في عملية الإدارة مما يسبب خسائر جسيمة للشركة أو المؤسسة.

- اختراق المواقع الإلكترونية والسيطرة عليها، ومن ثم توظيفها لتخدم مصالح كيانات خطيرة تهدف لزعزعة الأمن بالبلاد والسيطرة على عقول الشباب وتحريضهم للقيام بأعمال غير مشروعة.

تدمير النظم:

- يكون هذا النوع من التدمير باستخدام الطرق الشائعة وهي الفيروسات الإلكترونية والتي تنتشر في النظام وتسبب الفوضى والتدمير، ويتسبب ذلك في العديد من الخسائر المرتبطة بالملفات المدمرة ومدى أهميتها في إدارة وتنظيم الشركات والمؤسسات.
- او تدمير الخادم الرئيسي الذي يستخدمه جميع من بالمؤسسة من أجل تسهيل الأعمال، ويتم ذلك من خلال اختراق حسابات الموظفين بالمؤسسة الخاصة بالشبكة المعلوماتية للمؤسسة والدخول على الحسابات جميعاً في نفس ذات الوقت، ويتسبب ذلك في عطل تام للخادم مما يؤدي إلى تدميره وبالتالي تعطل الأعمال بالشركات والمؤسسات.

ثالثا: جرائم الأموال.

- **الإستيلاء على حسابات البنوك:** وهي اختراق الحسابات البنكية والحسابات المتعلقة بمؤسسات الدولة وغيرها من المؤسسات الخاصة، كما يتم أيضاً سرقة البطاقات الإئتمانية، ومن ثم الإستيلاء عليها وسرقة ما بها من أموال.
- **انتهاك حقوق الملكية الفكرية والأدبية:** وهي صناعة نسخ غير أصلية من البرامج وملفات المالتيميديا ونشرها من خلال الإنترنت، ويتسبب ذلك في خسائر فادحة في مؤسسات صناعة البرامج والصوتيات.

رابعا: الجرائم التي تستهدف أمن الدولة.

- **برامج التجسس:** تنتشر العديد من برامج التجسس والمستخدمة في أسباب سياسية والتي تهدد أمن وسلامة الدولة، ويقوم المجرم بزرع برنامج التجسس داخل الأنظمة الإلكترونية للمؤسسات، فيقوم أعداء الوطن بهدم أنظمة النظام والإطلاع على مخططات عسكرية تخص أمن البلاد، لذلك فهي تعتبر من أخطر الجرائم المعلوماتية.

- **استخدام المنظمات الإرهابية لأسلوب التضليل:** ويعتمد الإرهابيون على استخدام وسائل الإتصال الحديثة وشبكة الإنترنت من أجل بث ونشر معلومات مغلوطة، والتي قد تؤدي لزعزعة الإستقرار في البلاد وإحداث الفوضى من أجل تنفيذ مصالح سياسية ومخططات إرهابية، وتضليل عقول الشباب من أجل الإنتفاع بمصالح شخصية.

ثانيا: خصائص الجرائم الرقمية

لتحقيق الأمن الفكري في ظل الثورة الرقمية الحديثة، لابد من اتخاذ مجموعة من التدابير الاستباقية والاستشافية التي تشكل متكاملة: "استراتيجية لتحقيق الأمن الفكري والمجتمعي والمعلوماتي"

أهم خصائص الجزائم الرقمية في ما يلي:

1 -خفاء الجريمة وسرعة التطور في ارتكابها.

2 -اعتبارها الأقل عنفا في التنفيذ.

3 -جريمة عابرة للحدود السياسية والجغرافية.

4 -سرعة محو الدليل وتغييب الجناة.

5 -صعوبة الوصول إلى الدليل: بسبب برامج الحماية القوية وأساليب التمويه وتقنيات التشفير.

6 -صعوبة ضبط جرائم المعلوماتية وتوصيفها قانونيا: لأنها تقع في فضاء إلكتروني يتسم بالتغيير والديناميكية والانتشار الجغرافي العابر للحدود.

7 -فكرة الإختصاص والطبيعة الدولية للجرائم المعلوماتية: بسبب وقوع الجرائم من أطراف خارج الحدود، وهو ما يطرح الإشكال حول الاختصاص القضائي وما يتبع ذلك من إجراءات الملاحقة والتحري مع ضرورة احترام سيادة الدول.

ثالثا: استراتيجية الوقاية من الجرائم الرقمية

وفي هذا الصدد يستوجب على المجتمعات والدول إعادة النظر فـــي السياسات الأمنية والتعليمية وتحديثها بما يجعلـــها قادرة على استيعاب كافة المتغيـــرات الحديثة، وذات كفاءة عاليـــة في مجابهة الأنماط الجديدة للإنحرافات والجرائـــم الإلكترونية التي تتسم بخصائص أكثـــر دقة وذكاء وخفاء وســـرعة وتأثيـــرا على نفوس وعقول فئة الشباب خصوصا، الذين هم أكثر ضحايا هـــذه الوسائط الجديـــدة ومن أشد المتفاعلين معها .

لذلك نقترح

1 -تحديث اكبر للمنظومة القانونية المتعلقة بالجرائم والجنح والجنايات وتكييفها مع مستجدات الواقع التكنولوجي الجديد و المتجدد باستمرار.

2 -تكثيف برامج التكوين للهيئات التعليمية والأمنية والقضائية في مجال التكنولوجيا المعلوماتية والرقمية وتزويدهم بالمهارات اللازمة قصد التحيين الدوري لمعارفهم وتمكينهم من معالجة الوضعيات التي تعترضهم بكفاءة أكثر.

3- ترقية الثقافة الرقمية لدى المجتمع من خلال تكثيف الحصص والبرامج التي تشرح مخاطر التوظيف السيئ للتكنولوجيا على الأفراد والأطفال خصوصا، وأساليب التحايل الرقمي في شتى الميادين:

التجارة والأموال، الإبتزاز، انتحال الشخصية، التشهير، القرصنة، الاختراق، الألعاب، المواقع الجهادية والإباحية...الخ، مع تقديم إرشادات هامة حول الإجراءات اللازم اتخاذها للوقاية منها أو تدابير الحماية حال التعرض لمثل هذه الحالات.

4 -تكييف البرامج الدراسية مع تطور البيئة الرقمية خاصة في المراحل الابتدائية بإحلال مواد تُعنى بالوعي الرقمي والتربية التكنولوجية وتعليم التلاميذ الاستعمالات الجيدة والسليمة للتكنولوجيا وتحذيرهم من عواقب وخطورة التوظيف الخاطئ.

5 -ضرورة التركيز على التكوين المتخصص في "الإعلام الأمني" وترقية مهارات رجال الأمن في مجال التكنولوجيات بشكل مستمر لمواكبة التحديثات المستجدة.

6 -وضع إطار تعريفي شامل للجرائم الحديثة والمتعلقة بمخاطر الإنترنت وتوعية الآباء بمدى خطورتها وعواقبها وطبيعتها وآثارها النفسية والاجتماعية والأخلاقية والأمنية على أبنائهم.

7 -تنقيح وتهذيب المحتوى الإعلامي المقدم سواء على التلفزيون أو شبكات التواصل والإنترنت كحجب المواقع غير الاخلاقية.

9 -ضرورة الانتقال من الاستراتيجية الدفاعية إلى الاستراتيجية الوقائية الاستباقية، ومن الأمن الاجتماعي التقليدي إلى التفكير في الأمن الفكري والمعلوماتي والسايبراني، فمنطلق كل جريمة هو انحراف على مستوى الفكر.

10 -التسويق الإعلامي للقيم الوطنية وتشجيع الجمعيات الشبابية التي تعنى بقضايا الشباب وتطلعاتهم وإنشاء خلايا الاستماع والتوجيه والنصح للشباب بما فيهم المنحرف، وذلك للانتقال من دور المتلقي والمتأثر إلى دور المؤثر.

جريمة الدخول للمواقع والأنظمة والشبكات ووسائل تقنية المعلومات

الدكتورة منى كامل تركي
استاذة القانون الدولي العام الزائر جامعة الحسن
الأول سطات (مصر)

ملخص الدراسة

حاولت الدراسة توضيح ماهية الجريمة المتعلقة بالدخول والاعتداء على المواقع والأنظمة والشبكات ووسائل تقنية المعلومات بالقيام بإلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أية بيانات أو معلومات تمثل صوراً من صور الاعتداء على المواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات الإلكترونية سواء كان الدخول بتصريح مشروع وتم فيه تجاوز حد الدخول لتحقيق أغراض غير المصرح بها في واجباته الوظيفة حسبما تقرره القوانين والأنظمة والتعليمات أو الدخول غير المشروع بالدخول واتمام الجريمة وصولاً إلى ضرورة تشدد الرقابة والحماية السيبرانية والقانونية والإدارية على النظام الإلكتروني والوسائل المستحدثة في كافة الهيئات الحكومية والخاصة باعتبار أن الجرائم الإلكترونية مرتبطة بالتطور التكنولوجي الذي يستهدف من القائم بها حماية المصلحة العامة وخدمة المواطنين في ضوء القواعد القانونية النافذة

أوضحت الدراسة صورتي جرائم الاعتداء على المواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات الإلكترونية وأركان الجريمة مع العقوبة التي أقرها المشرع الإماراتي، وفقاً لقانون الجرائم الإلكترونية رقم (5) لعام 2012 والمعدل بقانون اتحادي رقم (12) لعام 2016 لمكافحة جرائم تقنية المعلومات ومجموعة المواد التي تتحدث بشكل مفصل عن الجريمة المتعلقة بالدخول والاعتداء على المواقع والأنظمة والشبكات ووسائل تقنية المعلومات بقانون تقنية المعلومات والجرائم الإلكترونية وقوانين الأمن السيبراني وعقوباتها في دولة الإمارات العربية المتحدة.

استخدمت الباحثة المنهج الوصفي التحليلي لشرح وتحليل النصوص القانونية محل التجريم في صورتيهما بمناسبة قيام الموظف أو بسبب تأدية عمله وتوصلت الدراسة إلى ضرورة تشدد الرقابة والحماية السيبرانية على الأنظمة الإلكترونية في كافة الهيئات الحكومية والخاصة باعتبار أن التحول الرقمي ضرورة حتمية مستمرة لتقنيات العمل الإلكتروني، والإدارة الإلكترونية، والحكومة الإلكترونية في كافة مجالات الأعمال الحكومية والخاصة أختتمت الدراسة بالنتائج والتوصيات

الكلمات المفتاحية: الحماية - الأنظمة التقنية - الشبكات - وسائل تقنية المعلومات- الرقابة – الأمن السيبراني- الجرائم الإلكترونية- التجريم – العقاب- الموظف.

Abstract

The study attempted to clarify; the nature of the crime related to accessing and attacking websites, systems, networks, and information technology means. by doing; By canceling, deleting, destroying, disclosing, destroying, altering, copying, publishing or re-publishing, any data or information, which constitute forms of attacking websites, systems, networks, or technical means Electronic information, whether the entry was with a legitimate permit, and the entry limit was exceeded, to achieve unauthorized purposes in his job duties, as determined by laws, regulations, and instructions, or illegal entry, by entering and completing the crime, up to the necessity of strict control and cyber protection, The legal, and administrative aspects of the electronic system, and the means developed in all governmental and private bodies, given that electronic crimes are linked to technological development, which aims to protect the public interest and serve citizens in light of the legal rules in force.

The study explained; Crimes of assault on websites, systems, networks, or electronic information technology means, and the elements of the crime with the penalty approved by the UAE legislator, in accordance with the Cybercrime Law No. (5) Of 2012 and amended by Federal Law No. (12) of 2016 to combat technical crimes Information, and a set of materials that talk in detail about the crime related to accessing and attacking websites, systems, networks, and information technology means, in the Information Technology and Cybercrime Law, and cybersecurity laws, and their penalties in the United Arab Emirates.

The researcher used; The analytical descriptive approach, to explain and analyze the legal texts subject to incrimination, in their two forms, on the occasion of the employee performing his work, or because of the performance of his work. The study found; to the need to tighten control and cyber protection on electronic systems, in all governmental and private agencies. Considering that digital transformation; imperative; ongoing e-work techniques, e-management, and e-government, in all fields of government and private business. The study concluded with results and recommendations.

Keywords: protection - technical systems - networks - means of information technology - control - cyber security - electronic crimes - criminalization - punishment – employee

المقدمة

مع استحداث أنظمة العمل والاعتماد على الأجهزة الإلكترونية ووسائل تقنية المعلومات واستخدام الكمبيوتر وشبكات الإنترنت في كافة الأعمال الحكومية والخاصة في الهيئات والوزارات والمدارس والجامعات وكافة مجالات الأعمال التجارية والمؤسساتية قد يقوم بعض الأفراد بأعمال غير مشروعة ينتج عنها جرائم مستحدثة في المجال الجنائي، فالجرائم الإلكترونية ارتبطت بالتطور التكنولوجي وأصبحت من أخطر الجرائم التي تواجهها الدولة وهي نوع من الجرائم مثل باقي الجرائم الأخرى قد توقع على شخص طبيعي أو اعتباري بل تنوعت وأصبح استخدام وسائل التكنلوجيا خطر على أمن الحكومات والمؤسسات والأفراد سواء كان محلياً أو دولياً حيث يقومون باستخدام التكنولوجيا لاختراق ونقل المعلومات للإضرار بالأشخاص وغيرهم.

فقد استلزمت نوعية الجرائم الإلكترونية اهتمام الدولة ومواجهتها بإصدار أحدث التشريعات في مجال تقنية المعلومات وذلك بالمرسوم بقانون اتحادي رقم 5 لسنة 2012 والمعدل بالقانون رقم (12) لسنة 2016 [138] بالإضافة إلى وضع الضوابط الضامنة للاستخدام الآمن والسليم للذكاء الاصطناعي والمواقع الحكومية والأنظمة والشبكات ووسائل تقنية المعلومات سواء كان الدخول بتصريح مشروع وتم فيه تجاوز حد الدخول لتحقيق أغراض غير المصرح بها في واجباته الوظيفة حسبما تقرره القوانين والأنظمة والتعليمات أو الدخول غير المشروع بقيام الموظف بعمل مخالفاً للقوانين والأنظمة بما يعرضه للمساءلة الجزائية وفقاً لقانون لمكافحة جرائم تقنية المعلومات الاتحادي ومجموعة المواد التي تتحدث بشكل مفصل عن إساءة استخدام الدخول بعد تحديد هوية الموظف والاعتداء على المواقع والأنظمة والشبكات ووسائل تقنية المعلومات وعقوباتها والجزاءات التأديبية للموظف وفقاً لقانون الموارد البشرية رقم 11 لسنة 2008 لدولة الإمارات العربية المتحدة وذلك لإحداث التوازن بين مصلحتين متضاربتين هي حماية مصلحة الموظف العام وبين حماية المصلحة العامة التي تمس كيان الدولة وخاصة في ممارسة الموظف لتطبيقات وممارسات الأنظمة الذكية بالعمل الحكومي أو الخاص.

لذلك سعت الباحثة لتوضيح ماهية الجرائم المتعلقة بدخول المواقع والأنظمة والشبكات ووسائل تقنية المعلومات باعتبار أن النظام الالكتروني يهم اغلبية الفئات ومصالح المجتمع والدولة اعتماداً على المنهج الوصفي

---

[138] () مرسوم بقانون 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات نشر بالجريدة الرسمية العدد 540 ملحق السنة الثانية والأربعون -بتاريخ 26-8-2012، والمعدل بالقانون الاتحادي رقم (12) لسنة 2016 الصادر بتعديل المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات بتاريخ 2016/5/23 والمعدل بالمرسوم رقم (2) لسنة 2018، والمنشور بالجريدة الرسمية العدد 633 السنة الثامنة والأربعون بتاريخ 2018/7/31.

التحليلي من خلال تحليل بعض من نصوص مواد التشريعات الاتحادية في مجال تقنية المعلومات، وقانون العقوبات، وتوضيح أركان الجريمة بعنصريها المادي والمعنوي والعقوبات المقررة عليها وذلك من أجل الوصول إلى الخلل ومحاوله علاجه بطريقه سليمه وتحديد صور الاعتداء ومصادرهم للتوصل إلى كيفية حماية بياناتهم من مثل هؤلاء الأشخاص وقسمت الدراسة في مبحثين نستعرض المبحث الأول يوضح ماهية جريمة تقنيه المعلومات ويوضح المبحث الثاني مواجهة جريمة تقنية المعلومات في الامارات.

أهمية الدراسة

تبرز أهمية الدراسة في توضيح ماهية الجرائم المتعلقة بدخول المواقع والأنظمة والشبكات ووسائل تقنية المعلومات في قانون تقنية المعلومات الاتحادي وقانون العقوبات باعتبار أن النظام الالكتروني يهم اغلبية الفئات ومصالح المجتمع والدولة بالإضافة إلى الأهمية التالية:

1. إن برامج المعلومات لها خصائص متميزة نظراً لطبيعتها الخاصة فتحتاج الحماية القانونية اللازمة لها.
2. فعل الدخول للمواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات سواء كان الدخول بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية أو شخصية قد يكون مشروعاً وقد يكون غير مشروعاً.
3. تتوافر المشروعية في الدخول للأشخاص المصرح لهم قانوناً، أما عدم المشروعية في حالة دخول الأشخاص المخترقين للمعلومات وهنا تتجه إرادة الجاني إلى فعل الدخول وهو يعلم بأنه ليس له الحق في الدخول إلى النظام والبقاء به.
4. أن المرسوم بقانون بشأن مكافحة جرائم تقنية المعلومات الإماراتي لم يعرف المقصود بالدخول، ولكنه قصد به الوصول إلى المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية، أو شبكة المعلومات، أو وسيلة تقنية معلومات، والعلم بمحتواها والسيطرة على المعطيات التي توجد بها أو الخدمات التي تقوم بها.
5. إن المعنى المادي لكلمة الدخول هو نشاط ذهني يقوم به الجاني للدخول، فالدخول هنا ذو طبيعة معنوية ويأخذ النشاط الإجرامي في هذه الجريمة صورة السلوك الإيجابي فإن الدخول غير المصرح به لا يتضمن الحالات التي تحدث صدفه.

6. جرم المشرع البقاء والاستمرار بصورة غير مشروعة داخل المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات أو وسيلة تقنية معلومات على غير المصرح به لحق الدخول المواقع والأنظمة والشبكات، ويقصد بالبقاء بصورة غير مشروعة، التواجد داخل المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات أو وسيلة تقنية معلومات على غير إرادة مالكها أو صاحب الحق في السيطرة عليها

مشكلة الدراسة

اختلفت الاحكام القانونية لجرائم الاعتداء على المواقع بين الصورة البسيطة في دخول موقع إلكتروني أو نظام معلوماتي إلكتروني، أو شبكة معلومات أو وسيلة تقنية معلومات، بدون تصريح وبين الصورة غير البسيطة في إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أية بيانات أو معلومات، مما يتضح **إشكالية الدراسة بطرح السؤال الرئيسي التالي:**

ما هي القواعد القانونية التي تحقق فعل تجريم الدخول إلى المواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات بتصريح تجاوز حد الدخول أو بدون تصريح؟

تساؤلات الدراسة

1. ماهية جريمة الدخول للمواقع في صورتها المجردة؟
2. ما هي أركان جريمة الدخول بدون تصريح؟
3. ما هي الصورة البسيطة لجرائم الاعتداء على المواقع بين الصورة البسيطة في دخول موقع إلكتروني، أو نظام معلوماتي إلكتروني، أو شبكة معلومات أو وسيلة تقنية معلومات، بدون تصريح؟
4. ما هي الصورة غير البسيطة في إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أية بيانات أو معلومات؟
5. ما هي الشروط الواجب توافرها لتوافر جريمة الاعتداء على المواقع بصورها البسيطة وغير البسيطة؟
6. كيف فرق المشرع الاتحادي بين جريمة الدخول بدون تصريح وبين جريمة تجاوز حدود تصريح الدخول؟
7. ما هي المواجهة التشريعية والقضائية في جريمة تقنية المعلومات؟

أهداف الدراسة

يكمن الهدف الرئيسي للدراسة في بيان الجرائم المتعلقة بدخول المواقع والأنظمة والشبكات ووسائل تقنية المعلومات واركانها والمواجهة التشريعية والقضائية لها بالإضافة إلى تحقيق الأهداف التالية:

1. أن جرائم الاعتداء على المواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات الإلكترونية تأخذ صورتين منها البسيطة وغير البسيطة مع توضيح الفرق بين جريمة الدخول بدون تصريح جريمة تجاوز حدود تصريح الدخول.
2. أن إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أية بيانات أو معلومات تمثل صوراً من صور الاعتداء على المواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات الإلكترونية.
3. التعرف على جرائم الاعتداء على المواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات الإلكترونية صورتين، صورة بسيطة وصورة غير بسيطة، مع بيان الركن المعنوي في مختلف الاعتداءات الماسة بالأنظمة المعلوماتية والذي يتخذ صورة القصد الجنائي، إضافة إلى نية الاعتداء من قبل الجاني وما يترتب عليه من عدم توافر أركان الجريمة إذا وقع الجاني في الخطأ سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء في نطاق هذا الحق، كأن يجهل بوجود حظر للدخول أو البقاء، أو كان يعتقد خطأ أنه مسموح له بالدخول.
4. التعرف على الشروط الواجب توافرها لجريمة الاعتداء على المواقع بصورها البسيطة وغير البسيطة في أن تكون هذه البيانات أو المعلومات شخصية، وأن يرتكبها الجاني في صورتيها بمناسبة أو بسبب تأدية عمله توضيح الفرق الاحكام القانونية، وأن تكون هذه البيانات أو المعلومات شخصية، وأن يرتكبها الجاني في صورتيها بمناسبة أو بسبب تأدية عمله.
5. التعرف على مواجهة جريمة تقنية المعلومات في الامارات واهتمام المشرع بالحيلولة دون قيام الجاني بهذا الفعل، وجرم نشاط الجاني الذي يتمثل في الدخول فيها بدون تصريح وذلك لتوفير الحماية الجنائية، وبهذا فإنه يستلزم لجريمة الدخول على المواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات بدون تصريح، أن يقوم الجاني بها مستخدماً حاسب آلي وشبكة معلوماتية، أو موقع إلكتروني، أو نظام معلوماتي، بالدخول إليها بدون الحصول على التصريح اللازم للدخول وبذلك يتحقق فعل الدخول إلى المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات أو وسيلة تقنية المعلومات.

منهجية الدراسة

استخدمت الباحثة المنهج الوصفي والتحليلي

(1)المنهج الوصفي :

في عرض صورتي جرائم الاعتداء على المواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات الإلكترونية مع العقوبة التي أقرها المشرع، وفقاً لنصوص مكافحة جرائم تقنية المعلومات والقانون الاتحادي رقم (12) لسنة 2016، الصادر بتعديل المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، قانون اتحادي رقم (1) لسنة 2006م في شأن المعاملات والتجارة الإلكترونية، وبالقانون رقم (5) لسنة 2017 بشأن تقنية الاتصال عن بعد في الإجراءات الجزائية، والقرار الوزاري رقم (259) لسنة 2019، في شأن الدليل الإجرائي لتنظيم التقاضي باستخدام الوسائل الإلكترونية والاتصال عن بعد في الإجراءات الجزائية ، والقرار الوزاري رقم (220) لسنة 2017 بشأن إنشاء نيابة جرائم تقنية المعلومات والصادر في 12 مارس 2017

(2) المنهج التحليلي:

لشرح وتوضيح النصوص القانونية محل التجريم بالاعتداء على المعلومات الإلكترونية المخزنة المواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات الإلكترونية في صورتيهما بمناسبة أو بسبب تأدية عمله لاي معلومات يمكن تخزينها ومعالجتها وتوليدها ونقلها بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والارقام والحروف والرموز والاشارات وغيرها

خطة الدراسة

مدخل تمهيدي: مفهوم الوظيفة في العمل الإلكتروني

المبحث الاول: ماهية جريمة الدخول للمواقع في صورتها المجردة

المطلب الاول: جريمة الدخول بدون تصريح وأركانها

المطلب الثاني: جريمة تجاوز حدود تصريح الدخول

المبحث الثاني: مواجهة جريمة تقنية المعلومات في الامارات.

المطلب الاول: المواجهة التشريعية في جريمة تقنيه المعلومات

المطلب الثاني: المواجهة القضائية في جريمة تقنية المعلومات.

مدخل تمهيدي: مفهوم الوظيفة في العمل الإلكتروني

تعد الوظيفة العامة من المواضيع الهامة في القانون كونها وسيلة من وسائل الإدارة العامة والتي تباشر مهامها وأنشطتها بواسطة أشخاص طبيعيين يمثلونها ويعملون لحسابها، وقد نظم القانون مركز الأشخاص القوانين والأنظمة المتعلقة بالوظيفة العامة وأعطى أهمية كبيرة للموظف العام لأن نجاح الإدارة في القيام بواجباتها يعتمد على كفاءة موظفيها وإحساسهم بالمسؤولية وضرورة تحقيق المصلحة العامة وقد نظم قانون العمل الاتحادي ومرسوم الموارد البشرية وتعديلاته [139].

الوظائف فى الوزارات ومصالحها والأجهزة الحكومية ووحدات الإدارة المحلية، والهيئات العامة، والمبادئ والأصول العامة الحاكمة للسياسات والتشريعات المتعلقة بالموارد البشرية على مستوى الحكومة وغايتها على وجه القطع واليقين والتأكيد على تحقيق الارتقاء بالمستوى الوظيفي ليكون مستهدفا العمل على تأكيد قيم المجتمع ومساهما في تنمية المهارات الوظيفية لأي من الموظفين ولضمان سير ونجاح وديمومة الوظيفة العامة وأنظمة العمل، وتضافر الجهود الداخلية للدولة وضمان تطبيق قانون إدارة الموارد البشرية على الدوائر الحكومة وأخلاقيات الوظيفة العامة والالتزام بمجموعة الآداب والقيم أو القواعد القانونية والأخلاقية للوظيفة العامة وتنظيم القواعد التي تحكم القيم الأساسية للموارد البشرية الحكومية بالدولة من حيث الالتزام بالمحافظة على الكرامة المهنية للوظائف العامة وعدم استغلال المنصب واستخدام الموارد بطريقة أصولية وعدم القيام بأي نشاط يؤثر على واجباته ومهامه الوظيفية وتجنب حدوث تضارب مصالح وفقاً لقانون الموارد البشرية الاتحادي [140].

ومع ثورة التقنية المعتمدة على الخدمات الإلكترونية والبريد الإلكتروني والأرشيف الإلكتروني والرسائل الصوتية والأدلة والمفكرات الإلكترونية ونظم المتابعة الإلكترونية والإدارة الإلكترونية والمؤتمرات الإلكترونية واستخدام التليفون المحمول أصبحت الخدمات الحكومية الإلكترونية تقدم بأسلوب جديد بسرية وأمن

---

[139]() قانون العمل الاتحادي رقم (8) لسنة 1980 وتعديلاته لعام 2012، والمرسوم بقانون اتحادي رقم (11) لسنة 2008 بشأن الموارد البشرية في الحكومة الاتحادية وتعديلاته بالمرسوم بقانون اتحادي رقم (9) لسنة 2011، والمرسوم بقانون اتحادي رقم (17) لسنة 2016

[140]() وفقاً للقانون الاتحادي رقم (5) لسنة 2017 بشأن تقنية الاتصال عن بعد في الإجراءات الجزائية، القرار الوزاري رقم (220) لسنة 2017 بشأن إنشاء نيابة جرائم تقنية المعلومات والصادر في 12 مارس 2017 أن الجهات المختصة الجهات الاتحادية أو المحلية المعنية بشؤون الأمن الإلكتروني في الدولة ، منى كامل تركي: النظام القانوني للإجازات في الوظيفة العامة، في التشريعات الاتحادية لدولة الإمارات العربية المتحدة، القاهرة، دار النهضة العربية، 2019، ص 18-19، إعاد حمود : الوجيز في القانون الإداري، دبي، أكاديمية شرطة دبي، ط1، 2004، ص205 خليفة خالد مرسي السليمان، التأديب في الوظيفة العامة وعلاقتها في قانون العقوبات، دراسة مقارنة، الأردن، الجامعة الأردنية، ط1، عام 2010، ص 152

المعلومات المتداولة في ظل التحول الرقمي وشملت العديد من الأعمال التي يقوم بها الموظف العام حسب القسم الذي يعمل به وحسب الدائرة الحكومية التي ينتمي إليها فألزم المشرع الاتحادي الجهات المختصة بالعمل بتقنية الاتصال عن بعد كإحدى الوسائل الفعالة التي تضمن الاستمرارية والارتقاء بالعمل الإلكتروني بتهيئة الموظفين بأنظمة الحاسب الآلي وتشغلها وسرعة التصرف بشأن أي مشكلة تواجه الموظف أثناء استخدام النظام المعلوماتي من حيث كشفها وضبط الأدوات التي استخدمت والتحفظ على البيانات أو الأجهزة التي استخدمت في ارتكابها أو تلك التي تكون محلا للجريمة على نحو يستدعى إعداد برامج تدريب وتأهيل لهذه الكوادر من الناحية الفنية بالكفاءة المطلوبة لمواجهة الأضرار بالأجهزة أو الملفات، أو المستندات الإلكترونية [141] لذلك أقتضت التعاملات في العالم الافتراضي بالتطبيقات الذكية إلى ضرورة إيجاد إطار تشريعي يحكمها وينظمها وقد تمثل ذلك في قانون مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة رقم (5) لسنة 2012 والمعدل بالقانون رقم (2) لسنة 2018، وقانون العقوبات الاتحادي رقم (4) لسنة 2019، والقانون رقم (5) لسنة 2017 بشأن استخدام تقنية الاتصال عن بعد في الإجراءات الجزائية [142]

فيكون الموظف أو المستخدم مسؤولاً مسؤولية كاملة عن العلم والعمل بالقوانين والأنظمة والقواعد والأحكام المتعلقة باستخدام النظام والتقييد بالآداب العامة والنظام العام وفقاً لأحكام وقوانين الدولة ويتعهد الموظف أو المستخدم بعدم انتحال أي صفة عند استخدام النظام، وعدم إدخال أو نشر أي محتويات غير قانونية تتضمن تمييزاً أو تشهيراً أو إساءة أو قذف أو سرقة الافكار أو سب أو فاحشة أو مواد إباحية أو محتويات تمس بالدين وبأحكام الشريعة الإسلامية أو الرموز أو السياسة العامة للدولة، عدم استخدام النظام لتحميل أي مادة فيها برامج تحتوي على فيروسات، أو ملفات أو برامج أو أجهزة قد تعمل على تغيير أو إتلاف أو إعاقة عمل النظام، عدم تغيير أو إتلاف أو شطب أي محتوى من محتويات الموقع أو التشجيع أو المشاركة بذلك، عدم خرق أو نشر أي مادة تتنافى أو تتعارض مع حقوق الملكية الفكرية للنظام الالكتروني وبحقوق الأخرين أو تخزين المعلومات الشخصية عن الآخرين ويتعهد الموظف أو المستخدم بالتزامه بمسؤوليته المسؤولية الكاملة عن جهاز

[141]() ومثالاً لذلك وجدت أجهزة الشرطة والتحقيق بالولايات المتحدة الأمريكية بعض الصعوبات هذا النوع المستحدث من التقنية سواء في كشف غموضها أو اجراء التفتيش والضبط اللازمين، أو التحقيق فيها على نحو استدعى إعداد برامج تدريب وتأهيل لهذه الكوادر من الناحية الفنية على نحو يمكنها من تحقيق المهمة المطلوبة منها وبالكفاءة المطلوبة هذه الاخطاء جسيمة ادت إلى الإضرار بالأجهزة او الملفات، أو الأدلة الخاصة بإثبات الجريمة

[142]() منى كامل تركي: الحماية الجنائية لحق الخصوصية في جرائم التصوير والتسجيل بدون إذن ووضع كاميرات المراقبة، وضوابط التوازن بين الحق في الخصوصية والضرورات الأمنية وفقاً لقوانين دولة الإمارات العربية المتحدة، القاهرة، دار النهضة العربية، ط1، 2018، ص 11-12

الحاسب الآلي المخصص له للدخول على المواقع والأنظمة الإلكترونية، فقد جـرم المشرع البقاء والاستمرار بصورة غير مشروعة داخل المواقع الإلكترونية أو أنظمة المعلومات الإلكترونيـــة أو شبكة المعلومات أو وسيلة تقنية معلومات على غير المصرح به لحق الدخول المواقع والأنظمة والشبــكات، ويقصد بالبقاء بصورة غير مشروعة، التواجد داخل المواقع الإلكترونية أو أنظمـــة المعلومات الإلكترونية أو شبكة المعلومات أو وسيلة تقنية معلومات على غير إرادة مالكها أو صاحب الحق في السيطـــرة عليها وسوف نوضح تلك الجرائم تفصيلاً في الدراسة.

المبحث الأول: ماهية جريمة الدخول للمواقع في صورتها المجردة

تمهيد وتقسيم

تعتبر تكنولوجيا المعلومات والمعرفة الركيزة الأساسية للتقدم والنمو فأصبحت العولمة حقيقة مؤكدة تتضمن شبكات مترابطة مترامية الأطراف تابعة لمؤسسات وهيئات متعددة الجنسيات، وشبكات إقليمية ودولية مرتبطة بالشبكة العالمية الإنترنت ويدار داخل الشبكات كافة العمليات الإدارية من مفاوضات وتخطيط وصفقات وبيع وشراء وتبادل خبرات وبحوث وفي ضوء العولمة انتشر الاقتصاد الشبكي والمنافسة وتزايد الضغوط على منظمات الأعمال لتحسين الأنماط الإدارية والأنظمة التي تستخدمها [(143)]

واتخذت جرائم الاعتداء على المواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات الإلكترونية صورتين صورة بسيطة وصورة غير بسيطة، فالصورة البسيطة تتمثل في دخول موقع إلكتروني، أو نظام معلوماتي إلكتروني، أو شبكة معلومات أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة، أما الصورة غير البسيطة تتمثل في إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أية بيانات أو معلومات، وأن تكون هذه البيانات أو المعلومات شخصية، وأن يرتكبها الفاعل في صورتيها بمناسبة أو بسبب تأدية عمله ووفقاً لنصوص المادتين 2، 3 من قانون جرائم تقنية المعلومات يمكن تقسيم الاحكام القانونية لجرائم الاعتداء على المواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات على النحو المبين في تقسيمنا للمطالب التالية:

---

[143]() علي عبد القادر القهوجي: الحماية الجنائية للبيانات المعالجة إلكترونياً، الإسكندرية، دار الجامعة الجديدة للنشر، ط1، 2006 ص 54 وما بعدها نائلة عادل محمد فريد قوره : جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقه، بيروت، منشورات الحلبي الحقوقية، ط1، 2005، ص 325 وما بعدها

المطلب الاول: جريمة الدخول بدون تصريح وأركانها

المطلب الثاني: جريمة تجاوز حدود تصريح الدخول

المطلب الأول: جريمة الدخول بدون تصريح وأركانها

حددت اللائحة التنفيذية الصادرة وفقاً لأحكام القانون بالمرسوم الاتحادي رقم (3) لسنة 2012 توفير الحماية الكافية فيما يتعلق بحقوق ومصالح المستفيدين من خدمات الاتصالات وتشـمل حماية البيانات وحماية الخصوصية على أن تكون مؤسسة الاتـصالات والأشخاص الاعتبارية الذين لهم الترخيص من قبل الهيئة وفقاً لأحكام القانون ولائحته التنفيذية وأن شبكة الاتصالات هي منظـومة تحتوي على جهاز أو وسيلة اتصال أو أكثر بهدف نقل أو بث أو تحويل أو استقبال أي خدمة من خدمات الاتصالات فإن فعل الدخول للمواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات سواء كان الدخـول بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية أو شخصية قد يكون مشروعاً وقد يكون غير مشروعاً [144].

وتقع على الموظف مسؤوليته عن اسم المستخدم الخاص به وجهازه المستخدم للدخول على النظام فيلتزم بعدم ترك الجهاز مفتوحاً على النظام في حالة قيامه من مكتبه، والالتزام بإغلاق النظام مجرد انهاء الغرض الذي فتح من أجله وعدم البقاء في النظام لغير الغرض المصرح به، وعدم تجاوز حد الدخول المصرح له وعدم الدخول على أقسام أخرى للاطلاع أو البحث عن غير المصرح له بالقيام به فالوصول إلى المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية، أو شبكة المعلومات، أو وسيلة تقنية معلومات، والعلم بمحتواها والسيطرة على المعطيات التي توجد بها أو الخدمات التي تقوم بها لكل نشاط ذهني يقوم به الموظف أو المستخدم لدخول موقع الكتروني أو نظام معلومات الكتروني أو شبكة معلومات أو وسيلة تقنية معلومات بدون تصريح وفقاً للمادة (2/تقنية المعلومات) [145]

---

[144]() المادة(1) من المرسوم بقانون اتحادي رقم (3) لسنة 2003، بشأن تنظيم الاتصالات المرسوم بقانون اتحادي رقم (3) لسنة 2003، والخاص بشأن تنظيم قطاع الاتصالات والمنشور بالجريدة الرسمية العدد 411 السنة 34 بتاريخ 2004/4/14 والمادة(1) من المرسوم بقانون اتحادي رقم (3) لسنة 2012 والخاص بإنشاء الهيئة الوطنية للأمن الإلكتروني والمنشور بالجريدة الرسمية بتاريخ 2012/8/13

[145]() المادة(2) من المرسوم بقانون لتقنية المعلومات بأن يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بأحدي العقوبتين كل من دخل موقعاً إلكترونياً أو نظاماً معلوماتياً أو شبكة معلومات أو وسيلة تقنية معلومات =

فإن مشروعية الدخول على الأنظمة إن كان الدخول للأشخاص المصرح لهم قانوناً وهم الموظفين بصفة عامة أو القائمين بالعمل في الأنظمة المعلوماتية أما عدم المشروعية في حالة دخول الأشخاص المخترقين للمعلومات وهنا تتجه إرادة الفاعل إلى فعل الدخول وهو يعلم بأنه ليس له الحق في الدخول إلى النظام والبقاء به وعلى ذلك اهتم المشرع بالحيلولة دون قيام الفاعل بهذا الفعل فقد جرم نشاط الجاني الذي يتمثل في الدخول فيها بدون تصريح وذلك لتوفير الحماية الجنائية ، وهنا حدد لجريمة الدخول بدون تصريح للدخول على المواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات أن يقوم الجاني بها مستخدماً حاسب آلي وشبكة معلوماتية، أو موقع إلكتروني، أو نظام معلوماتي، بالدخول إليها بدون الحصول على التصريح اللازم للدخول وبذلك يتحقق فعل دخول الأشخاص المخترقين للمعلومات إلى المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات أو وسيلة تقنية المعلومات [146] ونوضح أركان جريمة الدخول بدون تصريح كما يلي:

أركان جريمة الدخول بدون تصريح وتتمثل أركان جريمة الدخول بدون تصريح لأي من المواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات بتوافر محل الجريمة وهو المواقع أو الأنظمة أو الشبكات والركن المادي ويتحقق بفعل الدخول بدون تصريح والركن المعنوي يتحقق بتوافر القصد الجنائي ونوردها تفصيلاً كما يلي:

أولاً: محل الجريمة: حدد المشرع الإماراتي محل الجريمة في الفقرة الأولى من المادة(2) من قانون تقنية المعلومات، بأنها المواقع الإلكترونية أو الأنظمة المعلوماتية أو شبكة المعلومات أو وسائل تقنية المعلومات، وأوردت المادة تفصيلاً مجملاً لتعريف كل منها على حدة، ونوضح محل جريمة الدخول بدون تصريح في المحل التالي (1) المواقع الإلكترونية (2)نظام المعلومات الإلكتروني ، (3) الشبكة المعلوماتية، (4) وسيلة تقنية المعلومات كما يلي:

(1) المواقع الإلكترونية بأنها مكان إتاحة المعلومات الإلكترونية على شبكة المعلومات ومنها مواقع التواصل الاجتماعي، والصفحات الشخصية والمدونات[147]

أو تجاوز حدود التصريح، فالاعتداء على المواقع أو الأنظمة الإلكترونية أو شبكة المعلومات فعل مجرم، وتجريمه على حالة عدم وجود تصريح بالدخول، ولكن الشخص الذي تم التصريح له قد يتجاوز حدود التصريح

[146]() منى كامل تركي : الحماية الجنائية لحق الخصوصية في جرائم التصوير والتسجيل بدون إذن، مرجع سابق ص218 وما بعدها

[147]() مرسوم بقانون 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات مرجع سابق

(2) **نظام المعلومات الإلكتروني:** ويقصد به مجموعة برامج معلوماتية ووسائل تقنية المعلومات المعدة لمعالجة وإدارة وتخزين المعلومات الإلكترونية أو ما شابه ذلك

(3) **الشبكة المعلوماتية:** ويقصد بها ارتباط بين مجموعتين أو أكثر من البرامج المعلوماتية ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات

(4) **وسيلة تقنية المعلومات:** يقصد بها أي أداة إلكترونية مغناطيسية، بصرية كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية، وأداء العمليات المنطقية والحسابية، أو الوظائف التخزينية، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر، تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية أو إيصالها للأخرين وبالتالي تقوم الجريمة عندما ينصب السلوك الإجرامي للجاني على المحل، ولا يلزم أن يقع السلوك على كل صور المحل، بل يكفي أن ينصب على إحداها فقط لقيام الجريمة [148]

ثانياً: الركن المادي للجريمة: يتجسد الركن المادي في جريمة الدخول بدون تصريح إلى المواقع الإلكتروني أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات، أو وسيلة تقنية معلومات، بوقوع فعل الدخول من الجاني أو الشخص مخترق الدخول بغير وجه حق إلى المواقع والقيام بكل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها ويتصف بعدم المشروعية المتمثلة في عدم الحصول على حق تصريح الدخول للمواقع فالسلوك الإجرامي للجريمة الذي يقوم به الفاعل من القيام بفعل الدخول والقيام بالدخول بدون تصريح[149] ونوردها تفصيلاً كما يلي:

(1) **فعل الدخول:** ويقصد به الوصول إلى المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية، أو شبكة المعلومات، أو وسيلة تقنية معلومات، والعلم بمحتواها والسيطرة على المعطيات التي توجد بها أو الخدمات التي تقوم بها، والقيام بنشاط ذهني يقوم به الجاني للدخول وليس نشاط مادي محض ولذلك يكون الدخول هنا ذو طبيعة معنوية ويأخذ النشاط الإجرامي في هذه الجريمة صورة السلوك الإيجابي، ويتضح من عبارات الفقرة

---

[148]() مادة (1) التعريفات من مرسوم بقانون 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات مرجع سابق ، منى كامل تركي: تقنية الاتصال عن بعد في إجراءات التحقيق الجنائي والتقاضي عن بعد، القاهرة، دار النهضة العربية، ط1، 2019، ص 42-43، عمر محمد أبو بكر بن يونس : الجرائم الناشئة عن استخدام الانترنت، الأحكام الموضوعية والجوانب الإجرائية، مرجع سابق ص 325 وما بعدها

[149]() أحمد فتحي سرور: الوسيط في قانون الإجراءات الجزائية، القاهرة، دار النهضة العربية، ط16، 2018، ص 468، منى كامل تركي: الحماية الجنائية لحق الخصوصية في جرائم التصوير والتسجيل بدون إذن، مرجع سابق ص219

الأولى من المادة(2) من المرسوم بقانون لتقنية المعلومات بقولها (كل من دخل ....)، وبناء على ذلك يمكن أن يقع فعل الدخول من أي شخص سواء كان يعمل في الجهة التي وقع فيها الدخول أو لا يعمل فيها وسواء كان محترفاً أم غير محترف، ولا يشترط أن يكون الدخول بطريقة معينة سواء حدث بالسطو على كلمة السر أو بفك الشفرة حيث جاءت عبارة نص المادة كعبارة مطلقة، دون تحديد طريقة بعينها وبالتالي فإن الدخول غير المصرح به لا يتضمن الحالات التي تحدث صدفه ولا يشترط توافر صفة معينة في الجاني الذي يقوم بفعل الدخول [150]

(2) عدم التصريح بالدخول: إن عدم وجود تصريح الدخول يعني عدم مشروعية دخول الجاني لعدم تمتعه بسلطة تمكنه وتعطيه حق الدخول فقيام الفاعل بالدخول وهو عالماً بأنه ليس له حق الدخول للأنظمة الإلكترونية وينصب السلوك الإجرامي لفعل عدم التصريح بالدخول أن يكون الجاني ليس له الحق في الدخول إلا بتصريح أي أنه شخص قام بالدخول على الأنظمة الإلكترونية إختراقاً لها دون أن يكون له حق الدخول أو لا يملك التصريح بالدخول الرسمى للأنظمة الإلكترونية مع علمه بذلك وقام بالفعل بإرادة تامة [151]

ثالثاً الركن المعنوي: يتكون الركن المعنوي للجريمة من مقومات بعضها نفسي وبعضها الأخر ذهني وتعتبر هذه المقومات المعنوية انعكاساً لماديات الجريمة في نفس الفاعل وتقوم من خلالها المساءلة الجنائية بعد أن تتوافر فيه أهليه العقوبة المقررة

القصد الجنائي: بإحاطة الجاني بعناصر الجريمة المادية كما حددها القانون مع اتجاه هذه الإرادة الآثمة لتحقيق عناصر الجريمة وحتى يتوافر القصد الجنائي يجب أن تتجه إرادته ونيته الإجرامية إلى الفعل وإلى النتيجة الإجرامية المترتبة عليه والعلم بمقومات الواقعة المنشئة للجريمة وذلك بعلم الفاعل بجميع المقومات المتعلقة بنشاطه الإجرامي والمقومات المادية المتصلة بسلوكه الإجرامي وما يحيط بسلوكه من ظروف مشددة من شأنها تغيير وصف الجريمة فالأصل عدم جواز الاعتذار بجهل القانون وبالتالي لا يجوز للجاني أن يدفع التهمه بعدم علمه بالقاعدة القانونية ويتطلب القانون العلم بكل المقومات التي تدخل في بنية الواقعة المكونة للجريمة كما حددها النص القانوني فيكفي بشأنها الدخول المجرد لكي تقع الجريمة، ويعد فعل الدخول من الأفعال

---

[150]() لم يعرف المرسوم بقانون بشأن مكافحة جرائم تقنية المعلومات الإماراتي المقصود بالدخول، ولا يقصد به المعنى المادي لكلمة الدخول، كأن يدخل الجاني المكان الذي يوجد به الحاسب الآلي بطريقة غير مشروعة ، منى كامل تركي: تقنية الاتصال عن بعد في إجراءات التحقيق الجنائي والتقاضي عن بعد، مرجع سابق ص 118.

[151]() فإن القصد بكلمة تصريح الدخول أن يكون الشخص الذي دخل الموقع أو الأنظمة الإلكترونية لديه صلاحية الدخول باسم المستخدم وكلمة المرور التي يحصل عليها بصفته موظف أو بصفته قائم على الأعمال في الأنظمة الإلكترونية

الإيجابية فإن قيام الجريمة يتوقف على إرادة الشخص القائم بالأعمال في الأنظمة الإلكترونية أو الجهة المنظمة للشبكة لأنهما يملكان السلطة والسيطرة على المواقع أو الأنظمة المعلوماتية وعلى ذلك تعد جريمة الدخول بدون تصريح إلى المواقع أو الأنظمة المعلوماتية من جرائم النشاط المجرد التي تقوم بمجرد ارتكاب فعل الدخول، دون النظر إلى تحقيق نتيجة معينة [152]

وقد يكون من الممكن ألا يعاقب علي فعل الدخول عندما يكون سلوك الشخص القائم بالأعمال في الأنظمة الإلكترونية أو الجهة المنظمة للشبكة سلوك مشروع حيث يكون سلوك مباح فلا تقوم المسؤولية الجنائية عن فعل مباح مثل حالات الدخول بتصريح من مالكي المواقع الإلكترونية أو الأنظمة المعلوماتية أو الشبكات فهي لا تحتاج إلى تصريح إذا كان سبب الدخول على المواقع والأنظمة للغرض المحدد مسبقاً وفي خلال مدة زمنية محددة لإتمام العمل دون تجاوز البقاء في المواقع والأنظمة وكذلك دون القيام بأي تصرف يتجاوز حد الدخول وحد العمل المصرح له به، وقد لا تتوافر أركان الجريمة إذا وقع الجاني في الخطأ سواء كان يتعلق بمبدأ الحق في الدخول بصفة وظيفته أو في البقاء في نطاق هذا الحق كأن يجهل بوجود حظر للدخول أو البقاء أو كان يعتقد بالخطأ أنه مسموح له بالدخول وفقاً لطبيعة الوظيفة القائم عليها، فالركن المعنوي في مختلف الاعتداءات الماسة بالأنظمة المعلوماتية يتخذ صورة القصد الجنائي إضافة إلى نية الاعتداء من قبل الجاني [153]

العقوبة المقررة: تضمنت المادة (2) من المرسوم بقانون اتحادي بشأن تقنية المعلومات ثلاثة صور لجرائم الإعتداء في صورتها البسيطة وهي جريمة الدخول بدون تصريح إلى مواقع أو أنظمة أو شبكات أو وسائل تقنية معلومات، وجريمة تجاوز حدود تصريح الدخول إلى مواقع أو أنظمة أو شبكات أو وسائل تقنية معلومات، جريمة البقاء بصورة غير مشروعة في مواقع أو أنظمة أو شبكات أو وسائل تقنية معلومات فقد قرر المشرع الإماراتي عقوبة الحبس والغرامة لكل من دخل موقع الكتروني أو نظام معلومات الكتروني أو شبكة معلومات ، أو وسيلة تقنية معلومات ، بدون تصريح أو بتجاوز حدود التصريح ، أو بالبقاء فيه بصورة غير مشروعة[154]

---

[152]() نائلة عادل محمد فريد قوره : جرائم الحاسب الآلي الاقتصادية، مرجع سابق ص 325 وما بعدها عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الانترنت، مرجع سابق ص 326 وما بعدها

[153]() المادة (7) تعديل أو اتلاف أو افشاء معلومات أو بيانات متعلقة بفحوصات طبية أو تشخيص طبي أو علاج بغير تصريح : يعاقب بالسجن المؤقت كل من حصل أو استحوذ أو عدل أو اتلف أو افشى بغير تصريح بيانات اي مستند الكتروني أو معلومات الكترونية عن طريق الشبكة المعلوماتية أو موقع الكتروني أو نظام المعلومات الالكتروني أو وسيلة تقنية معلومات وكانت هذه البيانات أو المعلومات تتعلق بفحوصات طبية او تشخيص طبي أو علاج أو رعاية طبية أو سجلات طبية .

[154]() المادة (2) مرسوم بقانون 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات: دخول موقع الكتروني او نظام معلومات الكتروني او شبكة معلومات او وسيلة تقنية معلومات بدون تصريح

المطلب الثاني: جريمة تجاوز حدود تصريح الدخول

إن الاعتداء على المواقع أو الأنظمة الإلكترونية أو شبكة المعلومات فعل مجرم، وتجريمه على حالة عدم وجود تصريح بالدخول، ولكن الشخص الذي تم التصريح له قد يتجاوز حدود التصريح وهو ما نصت عليه المادة(2) من المرسوم بقانون لتقنية المعلومات بأن يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بأحدي العقوبتين كل من دخل موقعاً إلكترونياً أو نظاماً معلوماتياً أو شبكة معلومات أو وسيلة تقنية معلومات أو تجاوز حدود التصريح ونوضح الجريمة كما يلي:

أولاً: أركان جريمة تجاوز مجال التصريح: اختراق المواقع أو النظام المعلوماتي بارتكاب الفاعل الجريمة أثناء أو بسبب تأديته عمله أو تسهيل ذلك للغير حيث يفترض ذلك أن الفاعل ليس مالكاً وليس له سلطة على الموقع أو وسيلة تقنية المعلومات وتم التصريح له بالدخول في مجالات محددة والقيام بأغراض معينة ولكنه تجاوز هذه الحدود بدخوله في غير المجالات المرخص له بدخولها قائماً بأغراض أخرى غير الأغراض التي كانت سبب التصريح فلا يقتصر الاعتداء على المواقع أو الأنظمة الإلكترونية أو شبكة المعلومات على عدم وجود التصريح بالدخول فقط ولكن قد يكون الشخص أو القائم بالأعمال مصرح له الدخول الفعلي للمواقع والأنظمة ولكن تصريحه للقيام بالعمل المكلف به فقط ولكنه تجاوزه باختراق المواقع أثناء أو بسبب تأدية عمله وعليه تتكون أركان الجريمة كما يلي:

الركن المادي للجريمة: يتجسد الركن المادي في جريمة تجاوز مجال التصريح إلى المواقع الإلكتروني أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات، أو وسيلة تقنية معلومات بوقوع فعل التجاوز من الفاعل وهو الشخص المصرح له بالدخول وتجاوز مجال تصريح الدخول بالبقاء فيه بصورة غير مشروعة أثناء أو بسبب تأدية عمله وأن يرتكبها القائم بالأعمال على الأنظمة الإلكترونية بمناسبة أو بسبب تأدية عمله. ووفقاً لنصوص المادتين 2، 3 من قانون جرائم تقنية المعلومات وهو السلوك الإجرامي في الجريمة.

فالشخص الذي صدر له تصريح الدخول ليس تصريح عام وإنما اقتصر على مجال محدد دون غيره حسب المهام الوظيفية التي يقوم بها بالتالي يكون دخول المجال المختص به في وظيفته مباح لا جريمة فيه، أما المجال غير المصرح بشأنه في دخوله يكون غير مشروع وذلك لأن كل موظف مكلف بتخصص مهني محدد فإن قام بدخول مجال غير المخصص له بوظيفته فيكون تجاوز حدود التصريح المتاح له ويحدث ذلك من العاملين في هذه المواقع أو الأنظمة أو الشبكة المعلوماتية لأنهم صرح لهم بالدخول فيها وقد يكون الدخول من أشخاص غير العاملين ومن أمثلة ذلك الأشخاص الذين يقومون بتصميم البرامج لتأدية مهام ومزودي خدمات

الشبكة فدخول هؤلاء الأشخاص على المواقع يعد جريمة ووفقاً للفقرة الأولى من المادة(2/ تقنية المعلومات) ويمكن أن يقع الدخول من أي شخص سواء كان يعمل في الجهة التي وقع فيها الدخول أو لا يعمل فيها وسواء أكان محترفاً أم غير محترف، ولا يشترط أن يكون الدخول بطريقة معينة فالنص مطلق دون تحديد طريقة بعينها [155]

فعل تجاوز غرض التصريح: فإن الفاعل لديه تصريح بالدخول ولكنه يستخـــدم التصريح في غـــرض غير الغرض الذي أعطى من أجله فالحق في الدخـــول الذي يتاج من الحصـــول على التصريـــح يجب أن يكون مقيداً بالغرض الوظيفي المحدد له فإذا تعارض الدخول مع غرض التصريـــح فإن الدخول يكون غير مشروع، ومثال ذلك التصريح لشخص بالدخول والحصول على معلومات عن حسابات مؤسسة معيـــنة فإذا به يحصل على معلومات تتعلق بمؤسسة أخرى أو بقســـم أخر أو بمعلومة أخرى عن متعامل أخر وهكذا وبذلك يكـــون قد تجاوز الغرض الأساسي المحدد له في مجال وظيفتـــه أو مجال عمله المحدد له مـــن الجهة المختصة.

وقد يرجع قيام الفاعل بالدخول غير المشروع إلى موقع إلكتروني بنظام معلومات الكتروني أو شبكة معلوماتية أو وسيلة تقنية معلومات لإرتكاب فعل إجرامي معين عالماً به وبإرادته التامة بالقيام سواء كان الدخول بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية أو الدخول إلى موقع إكتروني لتغيير تصاميم هذا الموقع، أو تلافه، أو تعديله، أو شغل عنوانه بالغاء أو حذف أو تدمير أو إفشاء أو اتلاف أو تغيير أو نسخ أو نشر أو اعادة نشر اي بيانات أو معلومات وفي هذه الحالة يكون الدخول من الأشخاص الذين يقومون بتصميم المواقع والبرامج لتأدية مهام معينة أو المستخدمون من الأفراد المسجلين بالمواقع والمصرح لهم بالدخول باسم مستخدم وكلمة مرور [156]

فعل البقاء بصورة غير مشروعة: جرم المشرع البقاء والاستمرار بصورة غير مشروعة داخل المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات أو وسيلة تقنية معلومات على غير إرادة المالك أو من له الحق في السيطرة على هذه المواقع والأنظمة والشبكات، ويقصد بالبقاء بصورة غير مشروعة، التواجد

[155]() محمود نجيب حسني : شرح قانون العقوبات، القسم العام، القاهرة، دار النهضة العربية، ط8، 2017، ص 645 وما بعدها، منى كامل تركي: تقنية الاتصال عن بعد في إجراءات التحقيق الجنائي والتقاضي عن بعد، مرجع سابق ص 118، عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الانترنت، الأحكام الموضوعية والجوانب الإجرائية، مرجع سابق ص 326 وما بعدها

[156]() محمد حسين منصور : الاثبات التقليدي والالكتروني، الإسكندرية، دار الفكر الجامعي ، ط1، 2010 ص21. نائلة عادل محمد فريد قوره : جرائم الحاسب الآلي الاقتصادية، مرجع سابق ص 325 وما بعدها

داخل المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات أو وسيلة تقنية معلومات على غير إرادة مالكها أو صاحب الحق في السيطرة عليها فالبقاء يعني استمرار وعدم خروج الجاني وعدم قطع تواجده عند علمه أن وجوده غير مصرح به، وبالتالي غير مشروع فهذه الجريمة تقع منذ بداية الوقت الذي كان يجب فيه على الفاعل أن يخرج وهو وقت العلم، ومثال البقاء غير المصرح به كأن يكون قد تم التصريح لشخص ما بالدخول إلى موقع إلكتروني والاستفادة من خدماته خلال فترة زمنية معينة أو بعدد معين من الخدمات فإذا به يظل داخل الموقع بعد فوات الفترة الزمنية المحددة أو الاستفادة بأكثر من العدد المصرح به [157]

وكذلك أن يجد الفاعل نفسه داخل المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات أو شبكة المعلومات أو وسيلة تقنية معلومات دون قصد الدخول، وإنما عن طريق الصدفة وبدون إرادة منه ولكنه بعد اكتشافه أنه في الداخل يستمر ويظل في الوقت الذي كان يجب عليه الخروج، وباستمراره في البقاء على الرغم من معرفته أنه غير مصرح له بذلك يقع الفعل المجرم وتقوم مسؤوليته عن هذا الفعل وفعل البقاء يتصف بأنه ذو طبيعة مستمرة وهذا على خلاف فعل الدخول غير المصرح به فإنه فعل ذو طبيعة وقتية [158]

الركن المعنوي لجرائم الدخول في صورته المجردة: إن الركن المعنوي ضروري لقيام الجريمة لوجود العلاقة التي تربط بين شخصية الفاعل ومادية الجريمة ولتحديد ماهية العلاقـة والمسؤولية يجب تحديد ماهية الركن المعنوي للجريمة هل كانت جريمة قصديه أو غير قصديـــه لان هذه الماديات والأفعال يسبغ عليها المقنن الصفة الغير مشروعه لقيام الفاعل بإرادته فيحدد القانون النـــشاط في صورتيه أن تكون الإرادة متجهة إلى عناصر الركن المادي وهي الفعل والنتيجة وتسمى هنا بالقصد الجنائـي وأن تكون الإرادة متجهــة إلى السلوك الإجرامي دون النتيجة وهنا تسمى بالخطأ فالإرادة عنصر مشترك بين صورتي الركن المعنوي وهما العمد والخطأ غير العمدي وبالتالي فأن الركن المعنوي للجريمة لا يعدو كونه محض علاقة نفسية أو إرادية بين

---

[157]() المادة (2) مرسوم بقانون 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات: دخول موقع الكتروني أو نظام معلومات الكتروني او شبكة معلومات او وسيلة تقنية معلومات بدون تصريح يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات ، بدون تصريح أو بتجاوز حدود التصريح ، أو بالبقاء فيه بصورة غير مشروعة

[158]() إبراهيم محمود نجيب : أصول دراسات الأمن القومي، وأصول إدارة الدولة، الأردن، أكاديمية الإدارة والسياسات والدراسات، مجلة الجامعة الإسلامية للبحوث والدراسات الإنسانية، المجلد العشرون، العدد 2، يونيو 2012، ص 529- 530، علي عبد القادر القهوجي: الحماية الجنائية للبيانات المعالجة إلكترونياً، مرجع سابق ص 58 وما بعدها محمد حسين منصور : الاثبات التقليدي والالكتروني، مرجع سابق ص 35 وما بعدها

الفاعل والسلوك الإجرامي الذي قام به وحصر اتـــجاه إرادة الفاعل إلى تحقيـق الواقعة القانونية المنشئة للجريمة[159]

فلم يحدد المرسوم بقانون لتقنية المعلومات صورة الركن المعنوي للجرائم التي تقع على موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات في صورتها البسيطة المنصوص عليها في المادة(2) من المرسوم بقانون وحيث أن المشرع لم يحدد الركن المعنوي في الجريمة الدخول إلا إنه وضع قاعدة عامة لمعالجة هذه الحالة بنص صريح في المادة (43) من قانون العقوبات التي تنص على أنه يسأل الجاني عن الجريمة سواء ارتكبها عمداً أم خطأ ما لم يشترط القانون العمد صراحة وبالتالي يعاقب الجاني على الجرائم الواقعة على موقع إلكتروني أو نظام معلوماتي إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات في صورتها البسيطة سواء وقعت عمداً أم بطريق الخطأ [160]

القصد الجنائي: فإن فعل الدخول للمواقع الإلكترونية أو الأنظمة المعلوماتية أو الشبكات والاستمرار بالبقاء فيه دون القيام بأغراض الوظيفة المطلوبة فيتحقق القصد الجنائي للجريمة بالاستمرار بالبقاء بالمواقع دون وجه حق واستخدام الموقع من أجل ارتكاب جرم أو التورط بأي تصرف ينطوي عليه المسؤولية الجزائية وفقاً لإحكام وقوانين الدولة مثل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أية بيانات أو معلومات، أو معلومات شخصية، وأن يرتكبها الجاني بسبب تأدية عمله. ووفقاً لنصوص المادتين 2، 3 من قانون جرائم تقنية المعلومات فالوصول إلى المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية، أو شبكة المعلومات، أو وسيلة تقنية معلومات، والعلم بمحتواها والسيطرة على المعطيات التي توجد بها أو الخدمات التي تقوم بها لكل نشاط ذهني يقوم به الموظف أو المستخدم للدخول [161]

---

[159]() محمود محمود مصطفى السعيد : شرح قانون العقوبات، القسم العام، مطبعه جامعه القاهرة ،ط9 ، 1974، ص 424، محمود نجيب حسني : شرح قانون العقوبات، مرجع سابق ص 648 وما بعدها ، رمسيس بهنام: شرح قانون العقوبات العام، الإسكندرية، منشاة المعارف، ط1، 1971ص 880 وما بعدها

[160]() مادة (43) يسأل الجاني عن الجريمة سواء ارتكبها عمدا أم خطأ ما لم يشترط القانون العمد صراحة، من قانون العقوبات الاتحادي رقم (3) لسنة 1987 وفقاً لأحدث تعديلاته تم نشره في العدد رقم (182) من الجريدة الرسمية نشر بالجريدة الرسمية في 02 ديسمبر 1987 م العدد 281 - الجزء 14 ص 56371، والمعدل بموجب القانون رقم (34) لسنة 2005، والمعدل بموجب القانون رقم (7) لسنة 2016، والمرسوم بقانون اتحادي رقم (24) لسنة 2018.

[161]() نصت المادة(2) من المرسوم بقانون لتقنية المعلومات بأن يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بأحدي العقوبتين كل من دخل موقعاً إلكترونياً أو نظاماً معلوماتياً أو شبكة معلومات أو وسيلة تقنية
=

فالموظف أثناء ممارسة العمل بالأنظمة الذكية يلتزم بتنفيذ الواجبات العامة بدقة وبشكل جدير بالثقة والالتزام بتشغيل النظام واستخراج البيانات المطلوبة منه بنية حسنة وتقديم البيانات المطلوبة حسب الطريقة التي تريدها الجهة الحكومية التي يعمل بها الموظف فقد تورد البيانات والمعلومات مسجلة على دسك أو على سيد يروم (C-DROM) أو على الأقراص المغنطة، أو على ورق، وعليه كقائم بالعمل على الأنظمة الإلكترونية الالتزام بالمحافظة عليها خوفاً من إتلافها، أو محوها أو تعديلها ويمكن أن تثور مسؤوليته الجنائية إذا رفض القيام بالمهمة المكلف بها، أو أتلف عمدا البيانات المطلوب منه التعامل معها، أو أساء استخدام مكان حفظها أو قام بالتعديل فيها فضلاً عن التزام الموظف بأداء مهمته التي حددتها له الجهة الحكومية التي يعمل بها في الوقت المحدد دون تجاوز حد الدخول المصرح به كما يلتزم بالمحافظة على سر المهنة وفي حالة إفشائه السر يعاقب بالعقوبة المقررة لهذه الجريمة في خدمة المتعاملين من الجمهور في مكان عمله خلال ساعات العمل الرسمية وذلك بغرض استمرارية الخدمة العامة ولتحقيق المصلحة العامة [162].

المبحث الثاني: مواجهة جريمة تقنية المعلومات في الامارات.

تمهيد وتقسيم

أدركت حكومة دولة الإمارات ضرورة توفير بنية ذات مواصفات عالمية لإنجاح جهود التنمية الاقتصادية وضمان معدلات النمو المنشودة للاقتصاد المحلي، وذلك لما يتمتع به قطاع الاتصالات من أهمية كأحد الروافد الداعمة لبقية القطاعات الاقتصادية، وما يمثله كدافع رئيسي لجهود التنمية الوطنية، فقطاع الاتصالات يمثل العمود الفقري للعديد من المجالات الاقتصادية وانطلاقا لذلك سعت الدولة إلى توفير حماية أمنية متطورة، فأنشأت الهيئة الوطنية للأمن الإلكتروني ونظم المعلومات لتوفير الحماية الكافية فيما يتعلق بحقوق ومصالح المستفيدين من خدمات الاتصالات، ومع شيوع استخدام الكمبيوتر والانترنت والتطورات المتسارعة نتج عنها الأعمال غير المشروعة وخلق جرائم مستحدثة في المجال الجنائي، وعلى صعيد تطور التشريعات والقوانين التي من شأنها مواكبة التطورات اهتمت الدولة بمواجهتها بإصدار أحدث التشريعات في مجال تقنية المعلومات، وقد ارتأت الباحثة توضيح ذلك من خلال المطالب التالية:

معلومات أو تجاوز حدود التصريح، فالاعتداء على المواقع أو الأنظمة الإلكترونية أو شبكة المعلومات فعل مجرم، وتجريمه على حالة عدم وجود تصريح بالدخول، ولكن الشخص الذي تم التصريح له قد يتجاوز حدود التصريح

(162) James E. Macmillan, J. Douglas Walker, Lawrence P. Webster : A Guidebook for Electronique Court Filing, Copyright 1998 West Group, Inc. National Center for State Courts staff

المطلب الاول: المواجهة التشريعية في جريمة تقنيه المعلومات

المطلب الثاني: المواجهة القضائية في جريمة تقنية المعلومات.

المطلب الأول: المواجهة التشريعية في جريمة تقنيه المعلومات

حرصاً من المشرع الإماراتي على توفير الحماية الأمنية للأفراد وخصوصياتهم وحماية أمن الدولة من أي انتهاكات للبرامج المعلوماتية ووسائل تقنية المعلومات المعدة لمعالجة وإدارة وتخزين المعلومات الإلكترونية فقد سن التشريعات الاتحادية التي تناولت الضمانات القانونية لضبط التوازن بين الحق في الخصوصية والضرورات الأمنية والحق في المعلومات الشخصية وخصوصية البيانات الإلكترونية، والجرائم الماسة بأمن الدولة ومصالحها لمواجهة الخطر الماس بالنظام العام بصفة عامة باستخدام شبكة المعلومات أو وسائل تقنية المعلومات [163] وسوف نوضح ذلك في أولاً مكافحة جرائم تقنية المعلومات بإصدار التشريعات والقوانين ، وثانياً: تخصيص نيابة جرائم تقنية المعلومات.

ثالثاً: تنظيم قطاع الاتصالات والهيئة الوطنية للأمن الإلكتروني ، رابعاً: استحداث استخدام الكاميرات التليفزيونية كما يلي:

أولاً: مكافحة جرائم تقنية المعلومات بإصدار التشريعات والقوانين : اهتمت دولة الإمارات العربية المتحدة بمواجهة ومكافحة جرائم تقنية المعلومات من الناحية التشريعية وذلك بإصدار تشريعاتها مثل:

- القانون الاتحادي رقم (12) لسنة 2016، الصادر بتعديل المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات
- قانون اتحادي رقم (1) لسنة 2006م في شأن المعاملات والتجارة الإلكترونية
- القانون رقم (5) لسنة 2017 بشأن تقنية الاتصال عن بعد في الإجراءات الجزائية
- القرار الوزاري رقم (259) لسنة 2019 في شأن الدليل الإجرائي لتنظيم التقاضي باستخدام الوسائل الإلكترونية والاتصال عن بعد في الإجراءات الجزائية
- القرار الوزاري رقم (220) لسنة 2017 بشأن إنشاء نيابة جرائم تقنية المعلومات والصادر في 12 مارس 2017
- وتنفيذاً للمبادئ العامة التي جاء بها دستور دولة الإمارات والتي جاء بها قانون العقوبات الاتحادي رقم (3) وتعديلاته في عام 2016، وعام 2018، وما جاء بالمادة (378/ 43) عقوبات اتحادي والمواد المتعلقة بحماية

---

[163]() منى كامل تركي : الحماية الجنائية لحق الخصوصية في جرائم التصوير والتسجيل بدون إذن، مرجع سابق ص 168

حق المواطن والدولة في الأمان ومبدأ شرعية الجرائم والعقوبات، ومبدأ شخصية العقوبة، واحترام الإجراءات القضائية

فقد شرعت الدولة في المرسوم بقانون اتحادي رقم (5) لسنة 2012، والمعدل بالقانون الاتحادي رقم (12) لسنة 2016، بعقوبات الحبس والغرامة في الجرائم المتعلقة بدخول المواقع والأنظمة والشبكات ووسائل تقنية المعلومات وذلك في المادة (2) من ذات القانون، على أن تكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسون ألف درهم ولا تجاوز سبعمائة ألف درهم أو بأحدي العقوبتين، إذا ترتب على أي فعل من الأفعال المنصوص عليها بالفقرة (1) من المادة(2) إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات بالإضافة إلى أن تكون العقوبة الحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بأحدي هاتين العقوبتين إذا كانت البيانات أو المعلومات محل الأفعال الواردة بها أفعال شخصية، وقرر المشرع الاتحادي عقوبة الحبس والغرامة التي لا تقل عن مائتين وخمسون ألف درهم لكل من اعتدى على المواقع أو الأنظمة الإلكترونية أو الشبكة المعلوماتية أو وسائل تقنية المعلومات بأي صورة من صور الدخول بها سواء كانت صورة مجردة أو صورة مصحوبة بالاعتداء [164]

ثانياً: تخصيص نيابة جرائم تقنية المعلومات: خصصت نيابة جرائم تقنية المعلومات للتحقيق والتصرف ومباشرة الدعوى الجزائية في جرائم استعمال الشبكة المعلوماتية والاتجار بالبشر والترويج غير القانوني للأسلحة والذخيرة والمتفجرات والأموال الغير مشروعة، وما تقتضي مصلحة العمل إحالته إليها من جرائم تقنية المعلومات، وحرصت الدولة بقوانينها وتشريعاتها على الجمع بين الشق الجنائي لهذه الجرائم والتطبيقات القضائية وشق الحماية القانونية والضرورات الأمنية والحق في المعلومات الشخصية وخصوصية البيانات الإلكترونية [165]

ثالثاً: تنظيم قطاع الاتصالات والهيئة الوطنية للأمن الإلكتروني : فقد حدد المشرع قطاع لتنظيم الشبكات والاتصالات والهيئة الوطنية للأمن الإلكتروني وسائل استخدام أي جهاز أو وسيلة اتصال أو أكثر بهدف نقل أو بث أو تحويل أو استقبال أي من خدمات الاتصالات وذلك بواسطة أي طاقة كهربائية أو مغناطيسية أو اليكترومغناطيسية أو إلكترو كيميائية أو إلكتروميكانيكية وإنها تشغل بصورة حصرية لمصلحة

---

[164]() المادة(2) من المرسوم بقانون اتحادي رقم (5) لسنة 2012، بشأن جرائم تقنية المعلومات

[165]() منى كامل تركي: تقنية الاتصال عن بعد في إجراءات التحقيق الجنائي والتقاضي عن بعد، مرجع سابق ص99

شخص واحد أو مجموعة واحدة من الأشخاص تجمعهم ملكية مشتركة لخدمة حاجاتهم الخاصة فإن عملية ربط شبكات الاتصالات بأي وسيلة لتمكين مستخدميها من الاتصال مع مستخدمي ذات الجهة أو أي جهة أخرى أو لتمكينهم من الاستفادة من خدمات الاتصالات التي تقوم بتقديمها جهة أخرى [166]

رابعاً: استحداث استخدام الكاميرات التليفزيونية : وقد اتجهت وزارة الداخلية في الدولة إلى استحداث استخدام الكاميرات التليفزيونية والمثبتة في الكثير من الأماكن كبوابات الخروج والدخول لقسم الجوازات في جميع مطارات الدولة، والكثير من مراكز التسوق الكبرى والصغرى بالدولة وبعض الشوارع مكتظة الحركة بتطبيق نظام بصمة العين وبصمة الوجه، لإظهار هوية الشخص وذلك بالنظر إليها من خلال قاعدة بيانات مرتبطة مع بعضها بوسائط وروابط اتصالات كالألياف الضوئية والكوابل والأسلاك وغيرها من المعدات الملحقة بها كالمكرات وأجهزة التقوية ومجمعات التوصيل ومسارات الربط والجسور وغير ذلك من المسميات التي تحتاجها شبكات المعلومات [167]

ومع تطور استخدام الكمبيوتر والانترنت تطورت أساليب ارتكاب الجرائم الإلكترونية نتج عنها الأعمال غير المشروعة وخلق جرائم مستحدثة في المجال الجنائي، مما أصبح من الضرورة استخدام سلاح العلم والتكنولوجيا المتطورة للكشف عن الجناة الخارقين لهذه المعلومات أو المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات أو وسيلة تقنية المعلومات وكان ذلك باستخدام كاميرات المراقبة للأماكن العامة والخاصة، حرصاً بالدرجة الأولى على الحماية الأمنية وتأمين الممتلكات العامة والخاصة والطرق والشوارع والمباني الحكومية وغير الحكومية وتأمين حركة سير المرور والطرقات وتأمين العمال في أماكن العمل، وحماية حقوق العاملين وعدم اختراق خصوصيتهم إلا وفق ما تنص عليه اللوائح التنظيمية كنوع من الأمن الوقائي لأنها تساعد على كشف المخالفات، وقد تستخدم المراقبة الأمنية بالدوائر التليفزيونية المغلقة كدليل إثبات في بعض القضايا [168]

فالتقنية المتقدمة التي اتاحت للخارجين عن القانون خرق منظومات الحاسب الآلي بهدف السرقة أو تخريب المعلومات أو تدمير أجهزة الحاسوب وكان لابد من مواجهتها المواجهة القضائية والتشريعية لتحديد الإجراءات الدفاعية والوقائية لحمايتها من أية اختراقات وخلق أجواء أمنية للمعلومات تضمن الحفاظ عليها،

---

[166]() المادة (1) من المرسوم بقانون اتحادي رقم (3) لسنة 2003

[167]() منى كامل تركي: تقنية الاتصال عن بعد في إجراءات التحقيق الجنائي والتقاضي عن بعد، مرجع سابق ص 223

[168]() منى كامل تركي: الحماية الجنائية لحق الخصوصية في جرائم التصوير والتسجيل بدون إذن، مرجع سابق ص 136

فضلاً عن حماية أمن الدولة الداخلي والخارجي، وضبط التوازن بين حق المجتمع الإماراتي في كشف الحقيقة بشأن الجرائم وتقرير المسؤولية الجنائية والمدنية على الجناة في وسائل الإثبات الجنائي للوصول إلى اليقين القضائي بتطابق النموذج القانوني للجريمة وبين الوقائع الحقيقية في إقامة الدليل الجنائي ونسبته إلى فاعل معين.[169]

المطلب الثاني: المواجهة القضائية في جريمة تقنية المعلومات

اعتنق المشرع الاتحادي معيار الخصوصية في حماية الحياة الخاصة بصفة عامة أو حماية للمعلومات والبيانات الشخصية والخاصة لدخول أشخاص أخرين بغير وجه حق في المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات أو وسيلة تقنية المعلومات بدون تصريح، بتوفير حماية أمنية متطورة، فأنشأت الدولة الهيئة الوطنية للأمن الإلكتروني ونظم المعلومات لتوفير الحماية الكافية فيما يتعلق بحقوق ومصالح المستفيدين من خدمات الاتصالات، وعلى صعيد تطور التشريعات والقوانين التي من شأنها مواكبة التطورات اهتمت الدولة بمواجهتها بإصدار أحدث التشريعات في مجال تقنية المعلومات[170]

وبهذا فإنه يستلزم لجريمة الدخول على المواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات بدون تصريح، أن يقوم الفاعل بها مستخدماً حاسب آلي وشبكة معلوماتية، أو موقع إلكتروني، أو نظام معلوماتي، بالدخول إليها بدون الحصول على التصريح اللازم للدخول وبذلك يتحقق فعل الدخول إلى المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات أو وسيلة تقنية المعلومات فإلزم القائمون بالأعمال الإلكترونية في جميع الجهات الحكومية والخاصة بالحفاظ على سرية العمل، والتزام الموظف بالدخول للموقع كمستخدم للنظام، و مسؤولية الموظف عن استخدام أنظمة الاتصال الحكومي، إدخال البيانات والمعلومات، وعدم إساءة استخدام النظام بأي شكل من الأشكال الخضوع لرقابة الموقع، والالتزام بسرية المعلومات والبيانات المسجلة بالنظام، وحماية المعلومات والبيانات المسجلة بالنظام، ومسؤولية الموظف عن جهازه، والتزام الموظف بسياسة خصوصية النظام وجرم النشاط الذي يتمثل في الدخول لشبكات الاتصالات بدون تصريح وذلك لتوفير الحماية الجنائية، وعلى ذلك يفترض ذلك أن الجاني ليس مالكاً وليس له سلطة على الموقع أو وسيلة تقنية المعلومات

---

[169]() لؤي عبد الله نوح: مدى مشروعية المراقبة الإلكترونية في الإثبات الجنائي، وحجية مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، وعوامل حجية الصورة والصوت في الإثبات الجنائي، دراسة مقارنة، القاهرة، مركز الدراسات العربية للنشر والتوزيع، ط1، 2018، ص 11 علي عبد القادر القهوجي: الحماية الجنائية للبيانات المعالجة إلكترونياً، مرجع سابق ص 61

[170]() منى كامل تركي : الحماية الجنائية لحق الخصوصية في جرائم التصوير والتسجيل بدون إذن، مرجع سابق ص 168

وتم التصريح له بالدخول، في مجالات محددة، وتحقيقاً لأغراض معينة، ولكنه تجاوز هذه الحدود بدخوله في غير المجالات المرخص له بدخولها، تحقيقاً لأغراض أخرى غير الأغراض التي كانت سبب التصريح [171] ونوضح ذاك كما يلي:

(1) **الحفاظ على سرية العمل:** يلتزم الموظف باحترام والتقيد بمبادئ الخصوصية والسرية فيما يتعلق بالمعلومات العامة والمعلومات الشخصية، وعدم الكشف عنها أو استخدامها أو نسخها أو نقلها أو إزالتها إلا في سياق ممارسته لواجباته الوظيفية أو كما هو مسموح به بموجب القانون أو بتصريح خطي مسبق أو في حالة كأن الهدف من الكشف عنها الكشف عن جريمة تعرض مصلحة الجهة الحكومية التي يعمل بها للخطر أو الضرر وذلك بالإبلاغ عنها الى السلطة الرسمية المختصة، باتخاذ الخطوات اللازمة، إن وجدت وضمان معرفة الشخص المعني بالغرض الذي جمعت المعلومات لأجله، وبأسماء الأشخاص المطلوب تقديم تلك المعلومات إليهم واتخاذ الخطوات الكافية لضمان حماية المعلومات الشخصية عن طريق الاجراءات الاحترازية الأمنية كما هو مطلوب اتخاذها وفق الظروف وذلك ضد فقدان المعلومات أو الدخول إليها أو استخدامها أو تعديلها أو الكشف عنها إلا بتفويض من مسئولي جهة عمله المختصين، وأي سوء استخدام أخر لها والاحتفاظ بالمعلومات الشخصية بطريقة يمكن استردادها في الحال، ويمكن للشخص المعنى الحصول على نسخة من تلك المعلومات ويمكن تعديل تلك المعلومات إذا كانت غير صحيحة ويلتزم الموظف حتى بعد تركه الخدمة، بالحفاظ على سرية أية معلومات رسمية أو شخصية كان قد اطلع عليها بحكم وظيفته، ما لم يكن الكشف عنها مسموحاً به ص ارحة بموجب القانون أو العرف الوظيفي كما يلتزم الموظف بتسليم أية ممتلكات تخص الجهة الحكومية التي يعمل بها وثائق، ملفات، اشرطة، أقراص، وغيرها اليها عند انتهاء خدمته ويترتب على مخالفه الموظف لهذا الواجب تعرضه للمسؤولية التأديبية والمسؤولية الجنائية إذا يشكل إفشاء أسرار الوظيفة جريمة بنص قانون العقوبات الاتحادي وفقاً للمادة (4/تقنية معلومات)[172]

---

[171]() محمود نجيب حسني : شرح قانون العقوبات، مرجع سابق ص 645 وما بعدها، إبراهيم محمود نجيب: أصول دراسات الأمن القومي، وأصول إدارة الدولة، مرجع سابق ص 533 نائلة عادل محمد فريد قوره: جرائم الحاسب الآلي الاقتصادية، مرجع سابق ص 328 وما بعدها

[172]() المادة (4) دخول المواقع الالكترونية ووسيلة تقنية المعلومات للحصول على بيانات حكومية ومعلومات سرية بمنشأة : يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين الف درهم ولا تجاوز مليون وخمسمائة الف درهم كل من دخل بدون تصريح الى موقع الكتروني ، أو نظام معلومات الكتروني، أو شبكة معلوماتية أو وسيلة تقنية معلومات، سواء كان الدخول، بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية وتكون العقوبة السجن مدة لا تقل =

(2) التزام الموظف بالدخول للموقع كمستخدم للنظام: يستخدم النظام من خلال الموقع الالكتروني وفقاً لأحكام وشروط النظام بصفة مستخدم أو متعامل أو موظف وهو المعني بموضوع تسجيل الدخول للموقع ويتعهد المستخدم أو المتعامل أو موظف باستعمال النظام لأغراض مشروعة وللغاية التي وضع من أجلها فقط ووفقاً للأحكام والشروط بما لايتعارض مع التشريعات السارية ويكون المستخدم مسؤولاً مسؤولية كاملة عن العلم والعمل بكل القوانين والأنظمة والقواعد والأحكام المتعلقة باستخدام النظام ويلتزم بالتقييد بالآداب العامة والنظام العام وفقاً لإحكام وقوانين الدولة وفقاً للمادة (22/تقنية معلومات) [173]

(3) مسؤولية الموظف عن استخدام أنظمة الاتصال الحكومي: يلتزم الموظف بمسؤولية استخدام أنظمة الاتصال الحكومي بما في ذلك البريد الالكتروني وأجهزة الكمبيوتر والانترنت والهاتف فقط لما هو ضروري لأداء واجباته الوظيفية ووفقاً لسياسة جهة العمل ووفقاً للقانون والتقيد بكافة القوانين والقرارات وأية قواعد واجراءات تصدر عن الجهة الحكومية التي يعمل بها بخصوص شراء البضائع والخدمات والأعمال من قبل جهة عمله لضمان الاستخدام الأمثل للموارد المتاحة والإلتزام بالمحاسبية والقانونية والإنصاف والنزاهة في عملية الشراء التقيد التام بسياسة أمن المعلومات وفقاً للمادة (3/تقنية معلومات) [174]

(4) إدخال البيانات والمعلومات: يلتزم الموظف بمسؤولية بادخال البيانات والمعلومات حسب القسم الذي يعمل به للجهة الحكومية فلا يجوز أن يقوم بإدخال بيانات ومعلومات بالنظام نيابة عن موظف أخر أو مستخدم أخر لإدخال البيانات والمعلومات فكل موظف مسؤول عن جهازه المستخدم واسمه كمستخدم بالوقت والساعة والتاريخ، فاستخدام الموقع الالكتروني أو استعمال النظام من خلال الموقع أو البريد الالكتروني من قبل

عن خمس 5 سنوات والغرامة التي لا تقل عن خمسمائة الف درهم ولا تجاوز 2 مليون درهم ، اذا تعرضت هذه البيانات أو المعلومات للالغاء أو الحذف أو الاتلاف أو التدمير أو الافشاء أو التغيير أو النسخ أو النشر أو اعادة النشر، من مرسوم بقانون 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات

[173]() المادة (22) يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من استخدم ، بدون تصريح ، أي شبكة معلوماتية ، أو موقعا إلكترونيا ، أو وسيلة تقنية معلومات لكشف معلومات سرية حصل عليها بمناسبة عمله أو بسببه .

[174]() المادة (3) مرتكب الجرائم في البندين 1 و 2 من المادة 2 من هذا المرسوم بقانون اتحادي بمناسبة تأدية عمله : يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين الف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من ارتكب اي من الجرائم المنصوص عليها في البندين 1 و 2 من المادة 2 من هذا المرسوم بقانون بمناسبة أو بسبب تأدية عمله .

مستخدم النظام أو الموظف هو استعمال شخصي للنظام فيحظر على المستخدم أو الموظف السماح لأي شخص ثالث باستعمال بيانات التعريف الخاص به وفقاً للمادة (22/تقنية معلومات) [175]

(5) عدم إساءة استخدام النظام بأي شكل من الأشكال: يكون الموظف أو المستخدم مسؤولاً مسؤولية كاملة عن العلم والعمل بالقوانين والأنظمة والقواعد والأحكام المتعلقة باستخدام النظام والتقييد بالآداب العامة والنظام العام وفقاً لأحكام وقوانين الدولة ويتعهد الموظف أو المستخدم بعدم انتحال أي صفة عند استخدام النظام، عدم استخدام الموقع من أجل ارتكاب جرم أو تشجيع الآخرين على التورط في أي تصرف قد يعد جريمة أو ينطوي على مسؤولية مدنية أو مسؤولية جزائية وفقاً لإحكام وقوانين الدولة، عدم إدخال أو نشر أي محتويات غير قانونية تتضمن تمييزاً أو تشهيراً أو إساءة أو قذف أو سرقة الافكار أو سب أو فاحشة أو مواد إباحية أو محتويات تمس بالدين وبأحكام الشريعة الإسلامية أو الرموز أو السياسة العامة للدولة، عدم استخدام النظام لتحميل أي مادة فيها برامج تحتوي على فيروسات، أو ملفات أو برامج أو أجهزة قد تعمل على تغيير أو إتلاف أو إعاقة عمل النظام، عدم تغيير أو إتلاف أو شطب أي محتوى من محتويات الموقع أو التشجيع أو المشاركة بذلك، عدم خرق أو نشر أي مادة تتنافى أو تتعارض مع حقوق الملكية الفكرية للنظام الالكتروني وبحقوق الأخرين أو تخزين المعلومات الشخصية عن الآخرين وفقاً للمادة (22/تقنية معلومات)

(6) الخضوع لرقابة الموقع: يلتزم الموظف بالمسؤولية التامة عن استخدامه للموقع مع علمه بخضوع استعمال النظام للرقابة التقنية والرقابة الأمنية، حيث يتم إدارة الموقع من قبل الوزارة ويترتب على استعمال النظام من خلال الموقع أو البريد الالكتروني المسؤولية المدنية والجنائية لضمان إمكانية الدخول بشكل آمن إلى الموقع الالكتروني إذ أن النظام لا يهدف سوى لتطوير الخدمات المقدمة من الجهات الحكومية المختلفة والتواصل مع المتعاملين والموظفين وتتحمل إدارة الموقع والقائمين عليه المسؤولية، المادية أو المعنوية، عن أي انقطاع أو تأخير أو خلل في الموقع الالكتروني أو الخدمات الالكترونية المقدمة من خلاله[176]

(7)الالتزام بسرية المعلومات والبيانات المسجلة بالنظام: يتعهد الموظف أو المستخدم بعدم إفشاء أو استخدام أو سوء إستخدام أية معلومات سرية تتعلق بالجهة الحكومية التي يعمل بها أو أي جهة حكومية علم

---

[175]() المادة (22) يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من استخدم ، بدون تصريح ، أي شبكة معلوماتية ، أو موقعا إلكترونيا ، أو وسيلة تقنية معلومات لكشف معلومات سرية حصل عليها بمناسبة عمله أو بسببه .

[176]() علي عبد القادر القهوجي: الحماية الجنائية للبيانات المعالجة إلكترونياً، مرجع سابق ص 66 وما بعدها

بها من خلال استخدامه النظام أو من خلال تعامله مع أي من الجهات الحكومية إضافة لذلك التعهد بعدم الإعلان بوسائل الإعلام المختلفة سواء داخل الدولة أو خارجها عن السجلات المقدمة من خلال النظام مالم يتم أخذ الموافقة الخطية المسبقة من قبل الجهة الحكومية الاتحادية التي يعمل بها أو الوزارة التابعة لها الجهة الحكومية والمعنية وفي حال الإخلال في الإلتزامات الواردة يحق لإدارة الجهة الحكومية المعنية إتخاذ الإجراءات المناسبة بحق المخل بالتزاماتة منها سواء بعدم إستمراره في نفس القسم أو منع إستخدام والدخول للنظام كما شدد القانون على سرية المعلومات،إذ ألزم الموظف خلال فترة خدمته وبعد انتهائها، بالمحافظة على سرية المعلومات التي اطلع عليها بحكم وظيفته أو بسببها، وعدم الإفصاح عنها، مكتوبة كانت أو شفهية، وسواء كانت تتعلق بعمل الحكومة أو الدائرة التي يعمل لديها، أو بأي دائرة أخرى، ما لم يحصل على إذن خطّي مسبق من المدير العام، أو بناءً على طلب جهة قضائية، أو أي جهة حكومية توجب تشريعاتها الحصول على تلك المعلومات وفقاً للمادة (4/ تقنية معلومات) [177]

(8) حماية المعلومات والبيانات المسجلة بالنظام: يتعهد الموظف أو المستخدم بحماية أي أداة إلكترونية مغناطيسية، بصرية كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية، وأداء العمليات المنطقية والحسابية، أو الوظائف التخزينية، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر، تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية أو إيصالها للأخرين وحددت اللائحة التنفيذية الصادرة وفقاً لأحكام القانون بالمرسوم الاتحادي رقم (3) لسنة 2012 توفير الحماية الكافية فيما يتعلق بحقوق ومصالح المستفيدين وحماية البيانات، حماية الخصوصية، وفقاً لأحكام القانون ولائحته التنفيذية وحماية الدخول من أي شخص سواء كان يعمل في الجهة التي وقع فيها الدخول أو لا يعمل فيها وسواء أكان محترفاً أم غير محترف سواء حدث بالسطو على كلمة السر أو بفك الشفرة [178]

[177]() المادة (4) دخول المواقع الالكترونية ووسيلة تقنية المعلومات للحصول على بيانات حكومية ومعلومات سرية بمنشأة : يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين الف درهم ولا تجاوز مليون وخمسمائة الف درهم كل من دخل بدون تصريح الى موقع الكتروني ، أو نظام معلومات الكتروني، أو شبكة معلوماتية أو وسيلة تقنية معلومات، سواء كان الدخول، بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية وتكون العقوبة السجن مدة لا تقل عن خمس 5 سنوات والغرامة التي لا تقل عن خمسمائة الف درهم ولا تجاوز 2 مليون درهم ، اذا تعرضت هذه البيانات أو المعلومات للالغاء أو الحذف أو الاتلاف أو التدمير أو الافشاء أو التغيير أو النسخ أو النشر أو اعادة النشر .

[178]() المادة(2) من المرسوم بقانون لتقنية المعلومات بقولها (كل من دخل ....) المادة(1) من المرسوم بقانون اتحادي رقم (3) لسنة 2012، بشأن إنشاء الهيئة الوطنية للأمن الإلكتروني مؤسسة الاتصالات والأشخاص الاعتبارية الذين لهم الترخيص من قبل =

(9) مسؤولية الموظف عن جهازه: يتعهد الموظف أو المستخدم بالتزامه بمسؤوليته المسؤولية الكاملة عن جهاز الحاسب الآلي المخصص له للدخول على المواقع والأنظمة الإلكترونية، تقع على الموظف مسؤوليتـــه عن اسم المستخدم الخاص به وجهازه المستخدم للدخول على النظام فيلتزم بعـــدم ترك الجهاز مفتوحاً على النظام في حالة قيامه من مكتبه، والالتزام بإغلاق النظام مجرد انهاء الغرض الـــذي فتح من أجله وعدم البقاء في النظام لغير الغرض المصرح به، وعدم تجاوز حد الدخول المصـــرح له وعدم الدخول على أقسام أخرى للاطلاع أو البحث عن غير المصرح له بالقيام به فالوصول إلى المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية، أو شبكة المعلومات، أو وسيلة تقنية معلومات، والعلم بمحتواها والسيطـــرة على المعطيات التي توجد بها أو الخدمات التي تقوم بها لكل نشاط ذهني يقوم به الموظف أو المستخـــدم للدخول وفقاً للمادة (2/ تقنية معلومات) [179]

فقد جرم المشرع البقاء والاستمرار بصورة غير مشروعة داخل المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات أو وسيلة تقنية معلومات على غير المصرح به لحق الدخول المواقع والأنظمة والشبكات، ويقصد بالبقاء بصورة غير مشروعة، التواجد داخل المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات أو وسيلة تقنية معلومات على غير إرادة مالكها أو صاحب الحق في السيطرة عليها وألزم بعدم إدخال أو نشر أي محتويات غير قانونية تتضمن تمييزاً أو تشهيراً أو إساءة أو قذف أو سرقة الافكار أو سب أو فاحشة أو مواد إباحية أو محتويات تمس بالدين وبأحكام الشريعة الإسلامية أو الرموز أو السياسة العامة للدولة، وعدم استخدام النظام لتحميل أي مادة فيها برامج تحتوي على فيروسات، أو ملفات أو برامج أو أجهزة قد تعمل على تغيير أو إتلاف أو إعاقة عمل النظام، وعدم تغيير أو إتلاف أو شطب أي محتوى من محتويات الموقع أو التشجيع أو المشاركة بذلك، وعدم خرق أو نشر أي مادة تتنافى أو تتعارض مع حقوق الملكية الفكرية للنظام الالكتروني وبحقوق الأخرين أو تخزين المعلومات الشخصية عن الآخرين وأن يتعهد الموظف أو المستخدم بالتزامه بمسؤوليته المسؤولية الكاملة عن جهاز الحاسب الآلي المخصص له للدخول على المواقع

الهيئة وفقاً لأحكام القانون ولائحته التنفيذيةالمادة(1) من المرسوم بقانون اتحادي رقم (3) لسنة 2003، بشأن تنظيم الاتصالات وأن شبكة الاتصالات هي منظومة تحتوي على جهاز أو وسيلة اتصال أو أكثر بهدف نقل أو بث أو تحويل أو استقبال أي خدمة من خدمات الاتصالات

[179]() نصت المادة(2) من المرسوم بقانون لتقنية المعلومات بأن يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بأحدي العقوبتين كل من دخل موقعاً إلكترونياً أو نظاماً معلوماتياً أو شبكة معلومات أو وسيلة تقنية معلومات أو تجاوز حدود التصريح، فالاعتداء على المواقع أو الأنظمة الإلكترونية أو شبكة المعلومات فعل مجرم، وتجريمه على حالة عدم وجود تصريح بالدخول، ولكن الشخص الذي تم التصريح له قد يتجاوز حدود التصريح

والأنظمة الإلكترونية، وتقع على الموظف مسؤوليته عن اسم المستخدم الخاص به وجهازه المستخدم للدخول على النظام فيلتزم بعدم ترك الجهاز مفتوحاً على النظام في حالة قيامه من مكتبه، والالتزام بإغلاق النظام مجرد انهاء الغرض الذي فتح من أجله وعدم البقاء في النظام لغير الغرض المصرح به، وعدم تجاوز حد الدخول المصرح له وعدم الدخول على أقسام أخرى للاطلاع أو البحث عن غير المصرح له بالقيام به

(10) التزام الموظف بسياسة خصوصية النظام: يتعهد الموظف أو المستخدم بالالتزام بإحترام خصوصية معلومات وبيانات المستخدمين والمتعاملين من الجمهور في النظام الإلكتروني مثل اسم المستخدم أو المتعامل وعنوانه مسكنه وتاريخ ميلاده ونوعه ورقم هاتفه والفاكس الخاصة به وبريده الإلكتروني وغير ذلك من المعلومات التي يتم جمعها عند التسجيل لدخول النظام من المتعاملين من الجمهور أو استخدام أي من أدوات الموقع الإلكتروني فالمعلومات الشخصية المقدمة من المتعاملين من الجمهور الهدف منها التحقق من هويتهم وعلاقتهم بالخدمة التي يوفرها الموقع بموجب النظام الإلكتروني وأنظمة الجهة الحكومية صاحبة الموقع الإلكتروني وربطها بهويته الإماراتية والهوية الرقمية للوثوق في معلومة المتعاملين من الجمهور وللتوقيع على المستند الإلكتروني المقدم من طرفهم، ويلتزم الموظف أو المستخدم بعدم الإفصاح عن المعلومات والبيانات المسجلة أو نشر معلومات خاصة بالمتعاملين للعامة أو لزملائه الموظفين في أقسام أخرى بنفس الجهة الحكومية التي يعمل فيها بطريقة تحدد هوية المتعامل الخاصة دون تفويض خطي من قبل المتعامل بشخصه على جواز الإفصاح عن معلوماته من الجهة الحكومية نفسها

وقد سن المشرع الاتحادي في قانون مكافحة جرائم تقنية المعلومات عقوبات الحبس والغرامة على من دخل في نظام شبكات المعلومات الإلكترونية أو أي وسيلة تقنية معلومات بدون تصريح يخول له ذلك أو بأي صورة غير مشروعة في المواد (2، 3، 4، 5، 6، 7، 8، 9، 10، 11، 12، 13، 14، 15، 16، 17) وتناول هذه الجريمة من حيث محلها والسلوك الذي يقوم عليه الركن المادي وركنها المعنوي والعقوبة المنصوص عليها.[180]

وتطبيقاً لذلك قضت المحكمة الاتحادية العليا في الطعن رقم (64) لسنة 27 قضائية بتغريم كل من المتهمين خمسين ألف درهم ومصادرة الأجهزة المضبوطة عن استغلالهم بغير وجه حق لخدمة من خدمات الاتصالات وفي الطعن رقم (71) جزائي لسنة (27) قضائية، قضت بتغريم المتهم خمسين ألف درهم عن استخدامه أجهزة اتصالات بدون ترخيص من الهيئة واستعمال محطة إرسال لاسلكي وتركيب واستعمال جهاز

[180]() مرسوم بقانون 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات 2018

إرسال لاسلكي مخالفاً لأحكام المادة(50) وبمصادرة الأجهزة السلكية واللاسلكية (المادة 76) وغيرها من المعدات والادوات المستخدمة بالمخالفات للمرسوم بقانون أو لائحة التنفيذية أو الأنظمة أو القرارات أو التعليمات أو القواعد الصادرة بموجبهما[181]

الخاتمة

حاولت الدراسة بيان الجرائم المتعلقة بدخول المواقع والأنظمة والشبكات ووسائل تقنية المعلومات واركانها والمواجهة التشريعية والقضائية لها بالإضافة إلى توضيح الفرق بين جريمة الدخول بدون تصريح جريمة تجاوز حدود تصريح الدخول مع بيان الركن المعنوي في مختلف الاعتداءات الماسة بالأنظمة المعلوماتية والذي يتخذ صورة القصد الجنائي، إضافة إلى نية الاعتداء من قبل الجاني وما يترتب عليه من عدم توافر أركان الجريمة إذا وقع الجاني في الخطأ سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء في نطاق هذا الحق، كأن يجهل بوجود حظر للدخول أو البقاء، أو كان يعتقد خطأ أنه مسموح له بالدخول

وأوضحت الدراسة كيفية التعرف على الشروط الواجب توافرها لجريمة الاعتداء على المواقع بصورها البسيطة وغير البسيطة في أن تكون هذه البيانات أو المعلومات شخصية، وأن يرتكبها الجاني في صورتيها بمناسبة أو بسبب تأدية عمله توضيح الفرق الاحكام القانونية، وأن تكون هذه البيانات أو المعلومات شخصية، وأن يرتكبها الجاني في صورتيها بمناسبة أو بسبب تأدية عمله لذا سعت دولة الإمارات إلى سن تشريع قانون مكافحة الجرائم الإلكترونية، وقد سلطنا الضوء في هذا الموضوع على قانون الجرائم الالكترونية رقم (5) لعام 2012 والمعدل بقانون اتحادي رقم (12) لعام 2016، مجموعة من المواد التي تتحدث بشكل مفصل عن ماهية الجرائم الالكترونية وعقوباتها في الإمارات

يستلزم لجريمة الدخول على المواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات بدون تصريح، أن يقوم الفاعل بها مستخدماً حاسب آلي وشبكة معلوماتية، أو موقع إلكتروني، أو نظام معلوماتي، والدخول إليها بدون الحصول على التصريح اللازم للدخول وبذلك يتحقق فعل الدخول إلى المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات أو وسيلة تقنية المعلومات أو الدخول بتصريح ثم تجاوز حد الدخول، فقد جرم المشرع البقاء والاستمرار بصورة غير مشروعة داخل المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات أو وسيلة تقنية معلومات على غير المصرح به لحق الدخول المواقع والأنظمة والشبكات،

[181]() الاتحادية العليا أبوظبي مجموعة الأحكام الجزائية عن السنة 27 قضائية الصادرة في يونيو 2014

وقصد بالبقاء بصورة غير مشروعة التواجد داخل المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات أو وسيلة تقنية معلومات على غير إرادة مالكها أو صاحب الحق في السيطرة عليها

وهنا تقتضي الحاجة أن يكون القائمين بالأعمال الإلكترونية وموظفي الجهات الحكومية على درجة كبيرة من المعرفة بأنظمة الحاسب الآلي، وسرعة التصرف بشأن أي مشكلة تواجه الموظف أثناء استخدام النظام المعلوماتي من حيث كشف الاختراقات وضبط الأدوات التي استخدمت والتحفظ على البيانات أو الأجهزة التي استخدمت في ارتكاب الإختراق التي تكون محلاً للجريمة على نحو يستدعى إعداد برامج تدريب وتأهيل لهذه الكوادر من الناحية الفنية على نحو يمكنها من تحقيق المهمة المطلوبة منها وبكفاءة لمواجهة الأضرار بالأجهزة أو الملفات أو المعلومات أو البيانات المسجلة أو المستندات الإلكترونية لمواجهة الصعوبات التي يمكن أن تحدث جراء هذا النوع المستحدث من التقنية سواء في كشف الأخطاء التي يرتكبها الموظفين أو بإجراء التفتيش والضبط اللازمين على الأنظمة الإلكترونية بشكل يومي أو التأخير في تسجيل البيانات المطلوبة إلكترونيا

النتائج والتوصيات: توصلت الباحثة إلى النتائج التالية

1. أن المشرع الاتحادي حدد فعل الدخول للمواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات سواء كان الدخول بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية أو شخصية قد يكون مشروعاً وقد يكون غير مشروعاً
2. لتوافر المشروعية في الدخول للأشخاص المصرح لهم قانوناً، أما عدم المشروعية في حالة دخول الأشخاص المخترقين للمعلومات وهنا تتجه إرادة الجاني إلى فعل الدخول وهو يعلم بأنه ليس له الحق في الدخول إلى النظام والبقاء به
3. أن المرسوم بقانون بشأن مكافحة جرائم تقنية المعلومات الإماراتي لم يعرف المقصود بالدخول، ولكنه قصد به الوصول إلى المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية، أو شبكة المعلومات، أو وسيلة تقنية معلومات، والعلم بمحتواها والسيطرة على المعطيات التي توجد بها أو الخدمات التي تقوم بها
4. إن المعنى المادي لكلمة الدخول هو نشاط ذهني يقوم به الجاني للدخول، فالدخول هنا ذو طبيعة معنوية ويأخذ النشاط الإجرامي في هذه الجريمة صورة السلوك الإيجابي فإن الدخول غير المصرح به لا يتضمن الحالات التي تحدث صدفه

5. أن تجريم الدخول فيها بدون تصريح وذلك لتوفير الحماية الجنائية، وبهذا فإنه يستلزم لجريمة الدخول على المواقع أو الأنظمة أو الشبكات أو وسائل تقنية المعلومات بدون تصريح، أن يقوم الجاني بها مستخدماً حاسب آلي وشبكة معلوماتية، أو موقع إلكتروني، أو نظام معلوماتي، بالدخول إليها بدون الحصول على التصريح اللازم للدخول وبذلك يتحقق فعل الدخول إلى المواقع الإلكترونية أو أنظمة المعلومات الإلكترونية أو شبكة المعلومات أو وسيلة تقنية المعلومات
6. تقتضي الحاجة أن يكون القائمين بالأعمال الإلكترونية وموظفي الجهات الحكومية على درجة كبيرة من المعرفة بأنظمة الحاسب الآلي، وسرعة التصرف بشأن أي مشكلة تواجه الموظف أثناء استخدام النظام المعلوماتي من حيث كشف الاختراقات وضبط الأدوات التي استخدمت والتحفظ على البيانات أو الأجهزة التي استخدمت في ارتكاب الإختراق التي تكون محلاً للجريمة

التوصيات

1. ضرورة تشدد الرقابة والحماية السيبرانية على الأنظمة الإلكترونية في كافة الهيئات الحكومية والخاصة باعتبار أن التحول الرقمي ضرورة حتمية مستمرة لتقنيات العمل الإلكتروني، والإدارة الإلكترونية، والحكومة الإلكترونية في كافة مجالات الأعمال الحكومية والخاصة
2. مراجعة المشرع الاماراتي للسياسات التشريعية بصورة دائمة للتعديل عليها في حالة ظهور أي موضوع جديد يتعلق بهذه الجريمة.
3. تنمية قدرات الموظفين بمجال استخدام الذكاء الاصطناعي ورفع مهارات جميع الوظائف المتصلة بالتكنولوجيا لمعرفهم حقوقهم وواجباتهم في ممارسة العمل بالأنظمة الذكية وتنظيم دورات تدريبية للموظفين الحكوميين وإصدار قانون حكومي بشأن الاستخدام الآمن للذكاء الاصطناعي.
4. يجب نشر الوعي لدى الافراد لمعرفة كيفية التعامل مع هذه الجريمة
5. إعداد برامج تدريب وتأهيل للكوادر العاملة من الناحية الفنية على نحو يمكنها من تحقيق المهمة المطلوبة منها وبكفاءة لمواجهة الأضرار بالأجهزة أو الملفات أو المعلومات أو البيانات المسجلة أو المستندات الإلكترونية لمواجهة الصعوبات التي يمكن أن تحدث جراء هذا النوع المستحدث من التقنية سواء في كشف الأخطاء التي يرتكبها الموظفين أو بإجراء التفتيش والضبط اللازمين على الأنظمة الإلكترونية بشكل يومي أو التأخير في تسجيل البيانات المطلوبة إلكترونيا
6. يجب التعاون بين الدول والمؤسسات لمعرفة السياسة التشريعية المتبعة لمواجهة هذه الجريمة.

المراجع والمصادر

أولاً: الكتب

1. أحمد فتحي سرور: الوسيط في قانون الإجراءات الجزائية، القاهرة، دار النهضة العربية، ط16، 2018،
2. إعاد حمود : الوجيز في القانون الإداري، دبي، أكاديمية شرطة دبي، ط1، 2004،
3. خليفة خالد مرسي السليمان، التأديب في الوظيفة العامة وعلاقتها في قانون العقوبات، دراسة مقارنة، الأردن، الجامعة الأردنية، ط1، عام 2010
4. رمسيس بهنام: شرح قانون العقوبات العام، الإسكندرية، منشاة المعارف، ط1، 1971
5. علي عبد القادر القهوجي: الحماية الجنائية للبيانات المعالجة إلكترونياً، الإسكندرية، دار الجامعة الجديدة للنشر، ط1، 2006
6. عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الانترنت، الأحكام الموضوعية والجوانب الإجرائية، القاهرة، دار النهضة العربية، ط1، 2004
7. لؤي عبد الله نوح: مدى مشروعية المراقبة الإلكترونية في الإثبات الجنائي، وحجية مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، وعوامل حجية الصورة والصوت في الإثبات الجنائي، دراسة مقارنة، القاهرة، مركز الدراسات العربية للنشر والتوزيع، ط1، 2018
8. محمد حسين منصور : الاثبات التقليدي والالكتروني، الإسكندرية، دار الفكر الجامعي ، ط1، 2010
9. محمود محمود مصطفى السعيد : شرح قانون العقوبات، القسم العام، مطبعه جامعه القاهرة ،ط9 ، 1974
10. محمود نجيب حسني : شرح قانون العقوبات، القسم العام، القاهرة، دار النهضة العربية، ط8، 2017
11. منى كامل تركي: تقنية الاتصال عن بعد في إجراءات التحقيق الجنائي والتقاضي عن بعد، القاهرة، دار النهضة العربية، ط1، 2019
12. منى كامل تركي: الحماية الجنائية لحق الخصوصية في جرائم التصوير والتسجيل بدون إذن ووضع كاميرات المراقبة، وضوابط التوازن بين الحق في الخصوصية والضرورات الأمنية وفقاً لقوانين دولة الإمارات العربية المتحدة، القاهرة، دار النهضة العربية، ط1، 2018
13. منى كامل تركي: النظام القانوني للإجازات في الوظيفة العامة، في التشريعات الاتحادية لدولة الإمارات العربية المتحدة، القاهرة، دار النهضة العربية، 2019
14. نائلة عادل محمد فريد قوره : جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقه، بيروت، منشورات الحلبي الحقوقية، ط1، 2005

ثانياً: المجلدات

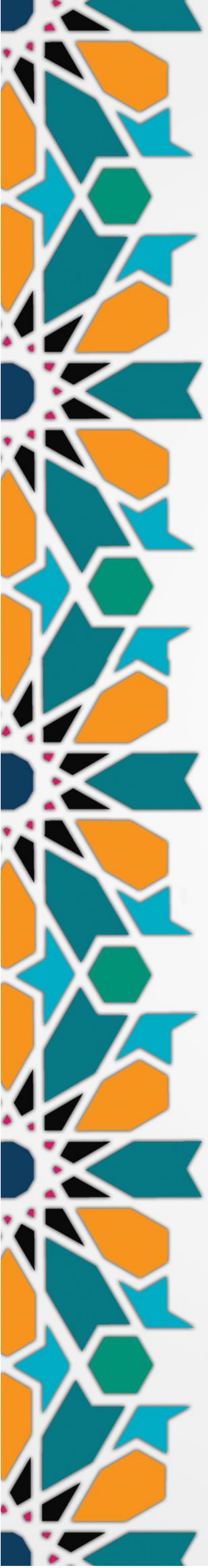
1. إبراهيم محمود نجيب : أصول دراسات الأمن القومي، وأصول إدارة الدولة، الأردن، أكاديمية الإدارة والسياسات والدراسات، مجلة الجامعة الإسلامية للبحوث والدراسات الإنسانية، المجلد العشرون، العدد 2، يونيو 2012، ص 529- 530

ثالثاً: القوانين والتشريعات

1. مرسوم بقانون 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات نشر بالجريدة الرسمية العدد 540 ملحق السنة الثانية والأربعون -بتاريخ 26-8-2012، والمعدل بالقانون الاتحادي رقم (12) لسنة 2016 الصادر بتعديل المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات بتاريخ 2016/5/23 والمعدل بالمرسوم رقم (2) لسنة 2018، والمنشور بالجريدة الرسمية العدد 633 السنة 48 بتاريخ 2018/7/31.
2. المرسوم بقانون اتحادي رقم (3) لسنة 2012، بشأن إنشاء الهيئة الوطنية للأمن الإلكتروني
3. المرسوم بقانون اتحادي رقم (3) لسنة 2003، بشأن تنظيم الاتصالات
4. قانون العمل الاتحادي رقم (8) لسنة 1980 وتعديلاته لعام 2012، والمرسوم بقانون اتحادي رقم (11) لسنة 2008 بشأن الموارد البشرية في الحكومة الاتحادية وتعديلاته بالمرسوم بقانون اتحادي رقم (9) لسنة 2011، والمرسوم بقانون اتحادي رقم (17) لسنة 2016
5. القانون رقم (5) لسنة 2017 بشأن تقنية الاتصال عن بعد في الإجراءات الجزائية
6. القرار الوزاري رقم (220) لسنة 2017 بشأن إنشاء نيابة جرائم تقنية المعلومات والصادر في 12 مارس 2017
7. المرسوم بقانون اتحادي رقم (3) لسنة 2003، والخاص بشأن تنظيم قطاع الاتصالات والمنشور بالجريدة الرسمية العدد 411 السنة 34 بتاريخ 2004/4/14 والمادة(1) من المرسوم بقانون اتحادي رقم (3) لسنة 2012 والخاص بإنشاء الهيئة الوطنية للأمن الإلكتروني والمنشور بالجريدة الرسمية بتاريخ 2012/8/13
8. قانون العقوبات الاتحادي رقم (3) لسنة 1987 وفقاً لأحدث تعديلاته تم نشره في العدد رقم (182) من الجريدة الرسمية نشر بالجريدة الرسمية في 02 ديسمبر 1987م العدد 281 - الجزء 14 ص 56371، والمعدل بموجب القانون رقم (34) لسنة 2005، والمعدل بموجب القانون رقم (7) لسنة 2016، والمرسوم بقانون اتحادي رقم (24) لسنة 2018.
9. الاتحادية العليا أبوظبي مجموعة الأحكام الجزائية عن السنة 27 قضائية الصادرة في يونيو 2014

رابعاً: المراجع الأجنبية

1. James E. Macmillan, J. Douglas Walker, Lawrence P. Webster : A Guidebook for Electronique Court Filing, Copyright 1998 West Group, Inc. National Center for State Courts staff



الجلسة العلمية الرابعة

رئيس الجلسة

الأستاذ عمر ابو الزهور

نقيب سابق بهيئة المحامين بمراكش

ربيع التحول الرقمي في دولة قطر بين التنمية الاقتصادية وتحديات الأمن السيبراني

الأستاذ مبارك السليطي
محام، عضو جمعية المحامين (قطر)

مقدمة :

في ظل التحول الرقمي الذي تشهده دولة قطر في الآونة الاخيرة، و الاعتماد المتزايد على تكنولوجيا المعلومات والاتصالات وشبكة الإنترنت ، مثل تطبيقات الهاتف النقال، واستخدم التكنولوجيا الرقمية في شتى مناحي الحياة اليومية، وتقديم الخدمات الحكومية عبر المنصات و التطبيقات الذكية إلى كافة المواطنين والمقيمين على أرض دولة قطر، الأمر الذي ولد العديد من الفرص للتطوير والابتكار، مما ينعكس على توفير العديد من الفرص الاستثمارية في العديد من القطاعات الحيوية لاسيما القطاع المالي وقطاعات الطاقة لتقديم خدمات فعالة وعالية الجودة والكفاءة

وعلى الرغم من ان التقدم الملحوظ في استخدام تكنولوجيا المعلومات واالاتصالات بما يحقق منافع اقتصادية هائلة للدولة، إلا انه يفرض في الوقت ذاته العديد من المخاطر والتي نتجت عن تعدد وتنوع االتهديدات الالكترونية التي تواجها الدولة في الآونة الاخيرة سواء على مستوى المؤسسات او الشركات او حتى الافراد، واصبحت الحاجة ماسة إلى أمن وامان فضائنا الالكتروني اكثر من اي وقت مضى، لاسيما مع تحديات انتشار جائحة كورونا، ومتطلبات الاتصال والتواصل بشكل آمن على شبكة الانترنت. وهو ما يستلزم تضافر وتعاون كافة مؤسسات الدولة وكافة الشركاء والفاعلين في وضع سياسة فاعلة للأمن السيبراني وحماية البنية التحتية المعلوماتية للدولة.

وفي إطار جهود دولة قطر لمواجهة هذه التحديات ومجابهة المخاطر والتهديدات الحالية والناشئة، وانطلاقًا من أهداف الاستراتيجية الوطنية للاتصالات وتكنولوجيا المعلومات 2015 الرامية إلى حماية البنية التحتية للمعلومات الحيوية الوطنية وتوفير بيئة آمنة لمختلف القطاعات لتقديم خدمات إلكترونية متكاملة، فقد تم وضع "الاستراتيجية الوطنية للأمن السيبراني" من قبل "اللجنة الوطنية لأمن المعلومات" التي أنشئت بموجب قرار

رئيس مجلس الوزراء رقم (18) لسنة 2013 لتوفير هيكل حوكمة للتعامل مع قضايا الأمن السيبراني بشكل جماعي على أعلى المستويات الحكومية.

لقد اهتمت العديد من دول العالم على اختلاف أنظمتها القانونية التي تنتهجها بصياغة تشريعات قانونية ولوائح تعالج العديد من الجوانب التي تتصل بالأمن السيبراني .. على سبيل المثال: حماية البيانات والخصوصية عبر شبكة الانترنت، والدخول الغير مصرّح به للمواقع الالكترونية ، والاستحواذ غير المشروع على البيانات.

وتقوم استراتيجية الأمن السيبراني والتي تم إنشاؤها من قِبَل اللجنة الوطنية لأمن المعلومات بموجب قرار رئيس مجلس الوزراء رقم (18) لسنة 2013 لتوفير هيكل حوكمة للتعامل مع قضايا الأمن السيبراني بشكل جماعي على أعلى المستويات الحكومية والعمل على تحقيق رؤية موحدة ومتكاملة تتمثل في تعزيز فضاء الكتروني آمن لحماية المصالح الوطنية لدولة قطر، والحفاظ على الحقوق والقيم الاساسية لمجتمعنا.

أهداف البحث :

وتهدف هذه الورقة البحثية إلى إلقاء الضوء على أبرز ملامح التطوّر التشريعي والتنظيمي في مجال تكنولوجيا المعلومات والاتصالات في ضوء الاستيراتيجية الوطنية التي اعتمدتها الدولة.. والوقوف على وضع استراتيجيات وسياسات وتشريعات مُضافاً إليها مجموعة من القواعد والإرشادات الخاصة بالأمن السيبراني لضمان تأمين أصول المعلومات، والتي تغطي كافة معاملات التجارة الإلكترونية، وأمن البنية التحتية لشبكة الإنترنت، وحماية البنية التحتية للمعلومات الحيوية هذا من جانب، ثم نعرض مدى قدرة التشريعات الوطنية المطبقة بالدولة على مواجهة تعدد وتشعب الجرائم الالكترونية في الآونة الاخيرة، والانتهاكات المتزايدة لأمن المعلومات وخصوصية البيانات الشخصية، ومظاهر الفراغ التشريعي في مواجهة الجريمة الالكترونية ، بالاضافة إلى كيفية استفادة دولة قطر من هذه التجارب في العديد من الأنظمة القانونية المقارنة في ضوء أفضل الممارسات الدولية من جانب آخر.

اشكالية البحث :

يعالج البحث العديد من الاشكاليات والتي ترتبط بالاطار القانوني والتنظيمي في مجال الأمن السيبراني، ومدى قدرة التشريعات المطبقة والسياسات التي انتهجتها دولة قطر على مواجهة التحديات يفرضها التحول

الرقمي في السنوات الاخيرة، لاسيما في ظل تعظيم الاستفادة من التطور التكنولوجي في مجال الاتصالات وتكنولوجيا المعلومات والذي تشهده الدولة في العديد من القطاعات الحيوية في ظل أفضل الممارسات الدولية.

استراتيجية الأمن السيبراني ومخاطر التجارة الالكترونية

لوحظ في الآونة الأخيرة ازدياد اعتماد الدول العربية على التجارة الالكترونية، في تقديم العديد من الخدمات عبر وسائل الانترنت والتي لها دور فعّال في الارتقاء بكفاءة الأعمال وزيادة فرص الاستثمار، مما ينعكس بالإيجاب على الاقتصاد الوطني لتلك الدول.

ومع ظهور جائحة كورونا -Covid 19- فقد اتجهت العديد من الشركات إلى تقديم خدماتها عن طريق منصّات التواصل الاجتماعي والتطبيقات الذكية، الأمر الذي فرض العديد من التحدّيات القانونية فيما يتعلق بكيفية حماية بيانات المستهلكين والشركاء وتأمين معاملاتهم في الفضاء الالكتروني. وهو ما تزامن مع التوسّع الملحوظ لدولة قطر في الآونة الاخيرة نحو استخدام التكنولوجيا الرقمية في العديد من الخدمات المالية والمصرفية، وهو يفرض التحدّيات بشأن استخدام المحفظة الالكترونية وبوابات الدفع الرقمية في ارتكاب جرائم انتحال الهوية عبر البريد الالكتروني، والنصب والاحتيال الالكرتوني، بالاضافة إلى جرائم غسل الأموال، والتي انتشرت بشكل ملحوظ في الآونة الأخيرة حسب تقارير وحدة الرقابة المالية.

وقد قطعت دولة قطر شوطاً كبيراً على الصعيد التشريعي والتنظيمي في مجال حماية الامن السيبراني للمستهلكين والتجار والمؤسسات المالية وكافة الأطراف ذات العلاقة، فعلى الصعيد التشريعي فقد نص قانون حماية خصوصية البيانات الشخصية على العديد من الضوابط القانونية التي يجب مراعاتها عند القيام بالاتصالات الالكترونية بغرض التسويق المباشر، حيث نصت المادة 22 من القانون على أنه " يُحظر إرسال أي اتصال إلكتروني بغرض التسويق المباشر إلى الفرد، إلا بعد الحصول على موافقته المسبقة. ويجب أن يتضمن الاتصال الإلكتروني هوية مُنشئه، وما يفيد بأنه مرسل لأغراض التسويق المباشر، كما يجب أن يتضمن عنواناً صحيحاً يسهل الوصول إليه، ويستطيع الفرد من خلاله أن يرسل طلباً إلى المنشئ بإيقاف تلك الاتصالات أو الرجوع في حال موافقته على إرسالها."

وقد تبنّت وزارة المواصلات والاتصالات -بوصفها الجهة المنوط بها تنظيم قطاع الاتصالات- المبادئ التوجيهية للتجارة الإلكترونية ، والتي تعدّ الأولى من نوعها بدولة قطر ، والتي هي نقلة نوعية تساعد التجار على المشاركة في بدء وتنفيذ أعمال التجارة الإلكترونية الناجحة. تأتي هذه المبادئ التوجيهية نتيجة تعاون

مشترك مع أصحاب المصلحة المحليين والإقليميين والدوليين عبر عمليات التجارة الإلكترونية بأكملها –بدءاً من إنشاء المنتج وحتى استلامه من قِبَل المستهلك. ويعتمد التنفيذ الناجح على التعاون والتنسيق القوي بين مختلف كافة الشركاء وأصحاب المصلحة.

كما تضمنت تلك المبادئ العديد من القواعد التي يجب على الشركات والمؤسسات اتباعها عند القيام بأي معاملات الكترونية ، والتي من بينها ادارة أصول المعلومات وتصنيفها واتخاذ التدابير الملائمة لمنع إساءة استخدامها من جهة والحفاظ على سريّتها وسلامتها وتوفرها بشكل مناسب، والعمل على تحقيق المتطلبات الأمنية لأنظمة المعلومات من جهة أخرى.

واستناداً إلى نص المادة 4، والمادة 5 من قانون الاتصالات رقم 34 لسنة 2006 والذي يخوّل المجلس الأعلى للاتصالات وتكنولوجيا المعلومات- بوصفه الجهة العليا المنوط بها تنظيم قطاع الاتصالات وتكنولوجيا المعلومات بدولة قطر – إصدار السياسات والتوجيهات الخاصة بهذا الشأن.

وانطلاقاً من أهمية الأمن السيبراني لمستخدمي خدمات الانترنت ،فقد قام المجلس الأعلى للاتصالات وتكنولوجيا المعلومات في عام 2013 بوضع الأحكام التي تعزز البنية التحتية لشبكات الانترنت بشكل تتسم بالمرونة والسلامة والأمن، وقامت بنشر إرشادات لأمن البنية التحتية لشبكة الانترنت على الموقع الرسمي لوزارة المواصلات والاتصالات.. والتي تهدف إلى حماية مستخدمي المنصات الافتراضية والمواقع الاليكترونية عند القيام بمعاملاتهم، بالإضافة إلى دعم ومساعدة مزوّدي الخدمة ومقدمي خدمات الاستضافة على تقديم خدمات الانترنت داخل دولة قطر بشكل آمن، وطبقاً للمتطلبات المعتمدة لمستوى الخدمة.

كما أدرك المجلس الأعلى للاتصالات وتكنولوجيا المعلومات أهمية حماية المستهلك من الرسائل الالكترونية التجارية والحد من مخاطر الرسائل الالكترونية الغير مرغوب فيها التي يتم انشاؤها أو استقبالها داخل دولة قطر ، ومن ثم فقد أصدر المجلس إرشادات بشأن مكافحة الرسائل الغير مرغوب فيها في عام 2013 والتي تشمل : رسائل البريد الاليكتروني، الرسائل النصية القصيرة SMS، والتسويق الصوتي عبر الهاتف، كما نص على شروط ومتطلبات إرسال الرسائل الالكترونية للأغراض التجارية داخل دولة قطر.

الأمن السيبراني وتحديات سلامة البيانات والمعلومات

مع تطور تكنولوجيا الاتصالات بدولة قطر، وتدفق البيانات عبر الحدود والذي يأتي مواكباً لتنظيم الدولة للعديد من الأحداث الرياضية الهامة وعلى رأسها بطولة كأس العالم لكرة القدم 2022 والذي أدى إلى تحوّل

جذريّ في مناخ الاقتصاد وزيادة حركة التجارة والاستثمارات بالدولة، وقد تضمن قانون خصوصية البيانات الشخصية رقم13 لسنة 2016 العديد من الالتزامات على عاتق الجهات والمؤسسات المخاطبة بأحكام هذا القانون عند معالجة البيانات الشخصية، وفرض عقوبات جنائية على مزوّدي الخدمة وكافة الأطراف المعنيّة عند مخالفة الالتزامات المنصوص عليها في هذا القانون، إلى جانب المسئولية الجنائية للمسئولين عن إدارة الأشخاص المعنوية.

وتأتي حماية النظم والبنية الأساسية لتكنولوجيا المعلومات والاتصالات على رأس أولويات الحكومة القطرية، فالفوائد العظيمة التي يقدمها لنا الفضاء الإلكتروني محفوفة بالعديد من التحديات التي قد تهدد البنية التحتية الحيوية، ومن أهم أهداف الاستيراتيجية الوطنية للأمن السيبراني هو الحفاظ على البنية التحتية الحيوية للدولة منها سبيل المثال: مرافق الكهرباء، والنقل، واستمرارية تشغيلها بشكل مستمر، وهو الأمر الذي يعزز من قدرتنا على الاستخدام الآمن للإنترنت.

وسعيًا منها لمواجهة هذه التحديات، تواصل دولة قطر بذل المزيد من الجهود الرامية إلى تعزيز الأمن السيبراني، فضلاً عن التعاون مع نظرائها حول العالم لخلق فضاء إلكتروني مفتوح وآمن. ومن أجل تحقيق هذه الغاية، فقد انشأت الوزارة "الفريق القطري للاستجابة لطوارئ الحاسب"، المعروف باسم "كيوسرت"، بالتعاون مع جامعة كارنيجي ميلون.

ويعمل قطاع الأمن السيبراني من خلال إدارتي "كيوسرت" و"حماية البنية التحتية للمعلومات الحيوية" مع الهيئات الحكومية وهيئات القطاعين العام والخاص والافراد على وضع آلية الرصد الإلكتروني لتفعيل وسائل الحماية الاستباقية وتطوير تطبيقات تحليل البرامج الخبيثة، كما يعمل القطاع على حماية المعلومات الحيوية على شبكة الإنترنت وضمان تأمينها من خلال اتخاذ الإجراءات اللازمة لتنفيذ إطار الاستجابة لاحتواء ودعم تعافي الأجهزة الحكومية وغير الحكومية من الأنشطة السيبرانية الضارة، بالتنسيق مع الجهات المختصة.

وطبقاً لأحدث احصائية صادرة عن الاتحاد الدولي للاتصالات ITU فإن 95% من مستخدمي شبكات الانترنت يتواجدون في دول لديها فريق وطني بشأن الاستجابة السريعة للهجمات الالكترونية CIRT، بالاضافة إلى اعتمادها استراتيجية وطنية للأمن السيبراني، وهو ما يدلل اهمية الجوانب التشريعية والتنفيذية معاً لاي دولة في حماية فضائها الالكتروني.

ويعد إصدار حزمة من السياسات والاجراءات الفعّالة لتأمين المعلومات الوطنية من أهم الخطوات الإيجابية التي اتخذتها وزارة الاتصالات، والتي تتضمن القواعد والأدوات ذات الصلة لتطبيق نظام آمن وفعّال لإدارة المعلومات الوطنية. وقد أصدرت وزارة المواصلات والاتصالات في اكتوبر من عام 2015 استراتيجية شاملة لتصنيف المعلومات الوطنية والتي تشمل سياسة تأمين المعلومات الوطنية وسياسة حماية البنية التحتية للمعلومات الحرجة.

وتتضمن هذه السياسة كتيّب عن الاجراءات الواجب اتباعها من كافة الجهات الحكومية والمؤسسات الخاصة بشأن تأمين المعلومات الوطنية، وتشمل بصفة رئيسية، الضوابط التي يجب مراعاتها من جانب كافة المؤسسات وتتمثل في متطلبات أمن الاتصالات و أمن الشبكات ، وضوابط تبادل المعلومات بين الجهات الحكومية وأمن النفاذ إلى بوابات الاتصالات، بالاضافة إلى القواعد التي يجب اتباعها في تكنولوجيا التشفير من أجل الحفاظ على سلامة وسرية المعلومات الخاصة والحساسة.

التكنولوجيا الرقمية في تقديم الخدمات المالية ومخاطر الأمن السيبراني

تعد قضايا الأمن السيبراني ومخاطر خرق البيانات وإفشاء سرية المعلومات، وغسيل الأموال من أبرز التحديات التي تواجه المؤسسات المالية والمصرفية، وهو ما قد يوثر على النظام المالي حسب ما أشارت إليه قمة العشرين التي عقدت بطوكيو، حيث بلغت خسائر خرق البيانات على مستوى القطاعات المالية حوالي 5.9 مليون دولار مقارنة 5.1 مليون دولار في عام 2015.

وحسب آخر احصائية صادرة عن شركة IBM والتي اظهرت أن 56% من الاختراقات الامنية في القطاع المالي كانت بسبب هجمات احتيالية، وطبقاً لآخر احصائية صادرة عن Deloitte بأن البنوك والمؤسسات المالية الكبرى قد انفقت ما يقارب من 15%من ميزانيتها على تطوير سياسات ومنظومات الأمن السيبراني لديها. كما بلغت تكلفة برامج الامتثال ومواجهة الجرائم في القطاع المالي في اوروبا والشرق الاوسط وشمال افريقيا في عام 2020 حوالي 117.5$ بليون دولار بزيادة بمعدل 21% عن العام السابق.

و مع زيادة استثمارات تكنولوجيا المعلومات في كافة الخدمات المالية والمصرفية، مع توقعات بزيادة مخاطر الهجمات الالكترونية ومخاطر خرق البيانات، وجرائم غسيل الأموال، يستعد مصرف قطر المركزي -بالتعاون مع مركز قطر للمال وكبرى المؤسسات المالية بالدولة- لنشر سياسة شاملة بشأن التكنولوجيا المالية) وذلك لتعظيم

استفادة القطاع المالي والمصرفي من التكنولوجيا الرقمية من جانب، ووضع إطار تنظيمي لهذه الخدمات المبتكرة، الامر الذي يسهم في تجنب مخاطر الأمن السيبراني المرتبطة بها من جانب آخر.

وقد وضّح قانون الجرائم الالكترونية عقوبات خاصة على مرتكبي هذه النوع من الجرائم ، وذلك بنصه في المادة 12 على أن" يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (200,000) مائتي ألف ريال، أو بإحدى هاتين العقوبتين، كل من ارتكب فعلاً من الأفعال التالية:

1- استخدام أو حصل أو سهل الحصول دون وجه حق على أرقام أو بيانات بطاقة تعامل إلكتروني عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.

2-زور بطاقة تعامل إلكتروني بأي وسيلة كانت.

3- صنع أو حاز بدون ترخيص أجهزة أو مواد تستخدم في إصدار أو تزوير بطاقات التعامل الإلكتروني.

4- استخدم أو سهّل استخدام بطاقة تعامل إلكتروني مزورة مع علمه بذلك.

5- قبول بطاقات تعامل إلكتروني غير سارية أو مزورة أو مسروقة مع علمه بذلك.

تحديات الأمن السيبراني في مجال العدالة الجنائية

تواجه التشريعات الخاصة بمكافحة الجرائم الالكترونية صعوبات عملية من ناحية ضعف الجوانب الاجرائية المتصلة بسلطات البحث والاستدلال، واجراءات التحقيقات التي تجريها النيابة العامة للحفاظ على الدليل الرقمي وكيفية إثباته وتقديمه للمحكمة الجنائية المختصة.حيث تقوم الجريمة الالكترونية على الدليل الرقمي والذي يختلف في شكله ومضمونه عن الدليل المادي في الجرائم بمفهومها التقليدي.

كما أن طبيعة الفضاء الإلكتروني- مترامية الاطراف- تتيح لبعض الجهات المغرضة فرصًا لاختراق بيانات الجهات الحكومية والخاصة افراداً او شركات وإلحاق الضرر بهم، لذا أصبح الحفاظ على سلامة أفراد المجتمع وشبكات البنية التحتية أحد أكبر التحديات العالمية التي تواجه جميع الدول، واصبح التعاون الدولي احد ابرز الحلول الناجحة لمواجهة مخاطر الأمن السيبراني والتصدي لمواجهة الجريمة الالكترونية عابرة للحدود

ومن ناحية أخرى، تعدّ مسألة التعاون الدولي بين الدول في مرحلة التحري وجمع الاستدلالات ومرحلة التحقيقات من المسائل التي تحتاج المزيد من الجهود على صعيد التشريعات العربية، والذي بات اليوم ضرورياً في الكشف عن ستر الجرائم الالكترونية وتقديم مرتكبيها للعدالة.

وحسب آخر احصائية صادرة عن الاتحاد الدولي للاتصالات بلغ اجمالي عدد الدول الموقعة على اتفاقيات ثنائية فيما يخص الأمن السيبراني 90 دولة بنسبة 46% من اجمالي دول العالم ، بينما بلغت النسبة المئوية للدول الموقعة اتفاقيات متعددة الاطراف بين الحكومات والمنظمات الاقليمية نسبة 57% من اجمالي الدول من بينها11 دولة عربية.

وعلى الرغم من عدم إنضمام قطر لاتفاقية بودابست لمكافحة الإجرام السيبيري ، إلا ان المشرع القطري قد استحضر روح الاتفاقية في نصوص قانون مستقل) قانون رقم 14 لسنة 2014 بشأن مكافحة الجريمة الالكترونية(، وقد عالج المشرع القطري كافة انواع الجرائم الالكترونية التي تضمنتها اتفاقية بودابست، وقام بتقسيم طوائف الجرائم الالكترونية إلى خمس طوائف رئيسية ، وقام بفرض عقوبات مغلّظة تشمل الحبس على مرتكبيها عند مخالفة الاحكام المنصوص عليها في هذا القانون .

وعلى سبيل المثال ، فقد فرض المشرع القطري عقوبة قد تصل إلى الحبس لمدة قد تصل إلى ثلاثة سنوات بالإضافة إلى الغرامة المالية في جرائم التعدي على انظمة وبرامج وشبكات المعلومات والمواقع الالكترونية، كما فرض عقوبات مغلّظة على كل من استغل الشبكة المعلوماتية او أحد وسائل تقنية المعلومات في نشر او بث او انتاج المحتوى الرقمي الغير مشروع ، والذي من شأنه تعريض سلامة وأمن الدولة للخطر، او يخالف القيم الاجتماعية والاخلاقية للدولة، بالاضافة إلى العقوبات التكميلية والتي تتمثل في حجب المواقع الالكترونية التي ارتكبت فيها او بواسطتها تلك الجرائم.

ومن ناحية أخرى ، فقد فرض القانون التزامات صارمة على مزودي الخدمة، ومن أهمها : تزويد الجهات المختصة، وجهات البحث والتحقيق والمحاكمة بجميع المعلومات والبيانات التي تساعده في كشف ستر الجرائم الالكترونية، والاحتفاظ المؤقت والعاجل ببيانات تقنية المعلومات أو بيانات المرور أو معلومات المحتوى لمدة تسعين يوماً قابلة للتجديد، بناءً على طلب الجهة المختصة أو جهات التحقيق والمحاكمة، بالاضافة إلى اتخاذ الإجراءات اللازمة لحجب روابط الشبكة المعلوماتية، بناءً على الأوامر الصادرة إليه من الجهات القضائية.

وانطلاقاً من أن طبيعة الجرائم الالكترونية بوصفها جريمة عابرة للحدود، فقد عالج قانون الجرائم الالكترونية – بشكل عام- العديد من الجوانب الهامة المرتبطة بالجريمة الالكترونية لاسيما فيما يخص اجراءات التحقيق، والتعاون الدولي بشأن مكافحة الجريمة الالكترونية، ، والتي في مجملها تتفق مع نصوص معاهدة بودابست للإجرام السيبيري، والتي تطرقت بشئ من التفصيل إلى الاجراءات الواجب اتباعها من جانب سلطات تنفيذ القانون في البحث والاستدلال ، وكيفية اثبات الدليل الرقمي و تقديمه للعدالة الجنائية، والاجراءات الضرورية للحفاظ على المعلومات وبيانات المرور، بالاضافة إلى آلية التعاون الدولي والمساعدة القضائية بين الدول لمكافحة الإجرام السيبيري.

فمن ناحية: فقد وضع القانون القطري قسم منفصل عن الاجراءات التي تقوم بها النيابة العامة في مرحلة التحقيقات ، ومن ناحية أخرى، فقد تطرق القانون إلى الاجراءات الخاصة بالتعاون الدولي والمساعدة القانونية المتبادلة، وقواعد تسليم المجرمين، والتي في مجملها لا تختلف عن تلك القواعد المنصوص عليها في قانون الاجراءات الجنائية.

ملخص البحث

لقد استعرض الباحث من خلال هذه الورقة أبرز ملامح التطوّر التشريعي والتنظيمي في مجال تكنولوجيا المعلومات والاتصالات في ضوء الاستراتيجية الوطنية للأمن السيبراني و التي اعتمدتها دولة قطر لضمان تأمين أصول المعلومات، والوقوف على وضع القواعد والإرشادات لأمن المعلومات، والتي تغطي كافة معاملات التجارة الإلكترونية، وأمن البنية التحتية لشبكة الإنترنت، وحماية البنية التحتية للمعلومات الحيوية، والصادرة عن وزارة المواصلات والاتصالات. ثم تناول الضوابط القانونية التي نص عليها قانون خصوصية البيانات الشخصية لحماية المعلومات والبيانات الشخصية للأفراد.

ثم تناول الدور الذي يقوم به مصرف قطر المركزي في وضع قواعد خاصة وإطار تنظيمي بشأن خدمات التكنولوجيا المالية(الفنتك)، الامر الذي من شأنه أن يسهم في تعظيم استفادة القطاع المالي من التكنولوجيا الرقمية من جانب، وحماية المؤسسات المصرفية من مخاطر التهديدات الالكترونية وخرق البيانات.

وقد عالج الباحث الطبيعة الخاصة للجريمة الالكترونية بوصفها جريمة عابرة للحدود من خلال العديد من الجوانب التي تعرض لها قانون الجرائم الالكترونية لاسيما فيما يخص طوائف هذه الجرائم ، وأهم العقوبات المفروضة على مرتكبيها، واجراءات التحقيق وجمع الاستلالات ، والتي في مجملها تتفق مع نصوص معاهدة

بودابست للإجرام السيبيري. كما شدد في الوقت نفسه على أهمية اثبات الدليل الرقمي و تقديمه للعدالة الجنائية، والاجراءات الضرورية للحفاظ على المعلومات وبيانات المرور، بالاضافة إلى آلية التعاون الدولي والمساعدة القضائية بين الدول لمكافحة الإجرام السيبيري.

الخاتمة والتوصيات :

لاشك أن الأمن السيبراني اصبح ضرورة ملحة في الوقت الحالي، خاصة مع التطور الهائل تكنولوجيا المعلومات والاتصالات، والاستفادة منها في كافة القطاعات الحيوية بالدولة، مما يتطلب تكاتف كافة الجهود والمبادرات بين كافة الشركاء حكومات و مؤسسات، وأفراد وشركات في إطار تنظيمي وتشريعي واضح يتوافق مع التطور السريع للهجمات الالكترونية ووسائل التعدي على انظمة وشبكات الاتصالات وامن المعلومات.

وقد حققت دولة قطر تقدماً ملحوظاً في وضع إطار قانوني وطني يوفر حوكمة متطورة للأمن السيبراني، ويحمي خصوصية البيانات والأفراد ، ويعزز مرونة البنية التحتية للمعلومات الحيوية. ويعد التعاون الدولي واتفاقيات المساعدة القضائية هو كلمة السر في مواجهة الاشكاليات التي تواجه سلطات انفاذ القانون في مواجهة الجرائم الالكترونية، وملاحقة مرتكبيها عبر الحدود .

ومن جماع ما تقدم يمكننا أن نوجز توصياتنا في النقاط التالية:

أولاً: الاستثمار بشكل فعال في الموارد البشرية ووضع السياسات والاجراءات التي تكفل تعزيز الأمن السيبراني للجهات الحكومية والخاصة والافراد بشكل فعال.

ثانياً : في إطار تنفيذها للسياسة الجنائية، مطالبة بالحرص على تحقيق الردع العام والخاص، لتحقيق الأمن المعلوماتي و حماية أمان المعاملات الإلكترونية، والحياة الخاصة للأفراد. وكل ذلك في حرص تام على تحقيق التوازن بين ردع الجريمة المعلوماتية واحترام الحقوق والحريات الأساسية للأفراد وعلى رأسها الحق في المعلومة وحرية التعبير والرأي.

ثالثاً: بناء منظومة قانونية متكاملة توازن بين التحول الرقمي الذي تشهده دولة قطر وبين وتوسيعِ نطاق المعاملات الإلكترونية من جهة، وبين حماية البنية التحتية المعلوماتية من كلَ الممارسات التي تهدد سلامة الأنظمة المعلوماتية بما يتناسب مع الاطار العام لقانون الاجراءات الجنائية القطري رقم 23 لسنة 2004 من جهة أخرى.

رابعاً: العمل على تطوير قدرات واثقال المهارات سلطات انفاذ القانون في مجال الادلة الجنائية، بما يدعم قدرتها على التحقيق في الجرائم الالكترونية والحفاظ على المعلومات وبيانات المرور، بما يتماشى مع الطبيعة الخاصة للدليل الرقمي والذي يحتاج تقنيات خاصة في اثباته والمحافظة عليه.

خامساً: تبني نظام سريع وفعال بشأن التعاون الدولي في مكافحة الجريمة الالكترونية، والتصدي للانتهاكات أمن وسرية المعلومات عن طريق تفعيل الاتفاقيات الثنائية أو الجماعية المبرمة بين دولة قطر وغيرها الدول على المستوى الاقليمي و الدولي، والانضمام إلى اتفاقيات ومعاهدات جديدة على سبيل المثال معاهدة بودايست بشأن الاجرام السيبري.

سادساً: الاستفادة من التجارب التشريعية للدول، والمنظمات الدولية والتي قطعت شوطاً في مجال الأمن السيبراني، على سبيل المثال: الاجراءات والقواعد التي تبنتها االأمم المتحدة ، ومفوضية الاتحاد الاوروبي في مجال مكافحة الاجرام السيبيري.

قائمة المراجع والمصادر

1.National Cyber Security Strategy, November 2014.Published on the website: https://www.motc.gov.qa/en/documents/document/national-cyber-security-strategy

2..Internet Infrastructure Security Guidelines, Supreme Council of Information & Communication Technology, Published on the website: https://www.motc.gov.qa/en/documents/document/internet-infrastructure-security-guidelines

3..Anti-Spam Guidelines, Supreme Council of Information & Communication Technology, published on : https://www.motc.gov.qa/en/documents/document/anti-spam-guidelines

4.. Convention on Cybercrime Budapest, 23.XI.2001

Published on official website https://www.coe.int/en/web/conventions/full-list//conventions/treaty/185?module=treaty-detail&treatynum=185.

5.Capacity Building on Cybercrime Country profiles of support provided by the Cybercrime Programm Office of the Council of Europe (C-PROC)

Published on : https://eucyberdirect.eu/wp-content/uploads/2020/06/compendium-capacity-building.pdf.

6.-International Cooperation against Cybercrime, European Council,

published on: https://www.coe.int/en/web/cybercrime/international-cooperation

7..Aigul Nukusheva, Roza Zhamiyeva, Viktor Shestak & Dinara, Formation of a legislative framework in the field of combating cybercrime and strategic directions of its development, Security Journal,2021

Published on: https://link.springer.com/article/10.1057/s41284-021-00304-3

8. Bill law, Gulf State Analytics Cybercrime laws and the GCC,

Published on : https://gulfstateanalytics.com/cybercrime-laws-and-the-gcc/

9.. Cybercrime Report Global Infographic July-December 2019.

Published on: https://risk.lexisnexis.com/global/en/insights-resources/infographic/cybercrime-report-infographic-july-december-2019.

10.International Telecommunication Union Development Sector, ITU Publications, Global Cybersecurity Index 2020 Published on: https://www.itu.int/en/publications/Pages/default.aspx

دور الحماية الجزائية للمعلوماتية في تحقيق الأمن السيبيراني

الدكتورة عبد الصدوق خيرة
أستاذة بكلية الحقوق و العلوم السياسية،
عضو في مخبر تشريعات حماية النظام البيئي-جامعة
ابن خلدون - تيارت (الجزائر)
Gmail: abdelsadokkheira@yahoo.fr

الملخص:

إن ظاهرة جرائم الكمبيوتر و الانترنت ، أو جرائم التقنية العالية ، أو الجريمة الالكترونية، ظاهرة إجرامية مستجدة نسبيا بحيث تعاني المجتمعات في الآونة الأخيرة من انتهاك للحقوق و الخصوصيات الالكترونية ، وذلك في ظل انتشار الجريمة الالكترونية و المعلوماتية ، وجاء تطور هذا النوع من الجرائم بالتزامن مع التطورات التي تطرا على التقنيات و التكنولوجيا التي يسرت سبل التواصل و انتقال المعلومات بين مختلف الشعوب و الحضارات و سهلت حركة المعلومات، فهي جريمة تقنية تنشأ في الخفاء و توجه للنيل من الحق في المعلومات المنقولة عبر نظم و شبكات المعلومات، وفي مقدمتها الانترنت، وتظهر مدى خطورتها في الاعتداءات التي تمس الحياة الخاصة للأفراد وتهدد الأمن بكل أنواعه والسيادة الوطنيين و تشيع فقدان الثقة بتقنية وتهدد إبداع العقل البشري .

الأمر الذي دفع بالدول إلى العمل مليا للحد من هذه الجرائم من خلال التوعية و الوسائل الوقائية الأمنية و غيرها، بحيث بات لزاما أن يواكب تطور الجريمة و أساليبها تطورا في مجال السياسة التشريعية عموما و السياسة الجنائية على وجه الخصوص، لهذا الاعتبار تكاثفت الجهود الدولية لمواجهة الآثار السلبية المترتبة على إساءة استخدام تقنية الاتصالات و المعلومات، لذا وجبة علينا الإلمام بالأحكام العامة لهاته الجرائم بتبيان مفهومها ثم التطرق إلى الحماية التي خصصها المشرع للحماية الجزائية للمعلوماتية في سبيل تحقيق الأمن السيبيراني.

Abstract

The phenomenon of computer and Internet crimes, or high-tech crimes, or cybercrime, is a relatively emerging criminal phenomenon so that societies have recently suffered from a violation of electronic rights and privacy, in light of the spread of electronic and information crime, and the development of this type of crime came in conjunction with The developments in techniques and technology that facilitated the means of communication and the transmission of information between different peoples and civilizations and facilitated the movement of information. It is transmitted through information systems and networks, foremost of which is the Internet, and shows the extent of its seriousness in attacks that affect the private lives of individuals and threaten security of all kinds and national sovereignty, and spread the loss of confidence in technology and threaten the creativity of the human mind.

Which prompted countries to work carefully to reduce these crimes through awareness and preventive security and other means, so that it became necessary to keep pace with the development of crime and its methods, a development in the field of legislative policy in general and criminal policy in particular, for this consideration intensified international efforts to confront the effects The negative consequences of the misuse of communication and information technology, so we have to be familiar with the general provisions of these crimes by clarifying their concept and then addressing the protection allocated by the legislator to the criminal protection of information in order to achieve cyber security.

مقدمة

يعتبر الأمن السيبيراني من أهم القضايا التي يجب أن تحتل الأهمية البالغة للمحافظة عل المجتمعات لما يشكله من خطر على جميع الأصعدة، حيث يعد الكمبيوتر من أبرز المستجدات التي أنتجتها التقنية في القرن الماضي . وهي تمر بثورة تعتمد على العلم والتقنية لتؤثر في جميع ميادين الحياة والتي ستقودنا إلى تطورات متعددة ومختلفة في شتى المجالات . فظهور الحاسب فرض كثيراً من المتغيرات في جميع النواحي المعرفية والعلمية حتى أصبحت بصمة الحاسب الآلي واضحة المعالم في جميع الميادين لتشكل أداة قوية لحفظ المعلومات ومعالجتها ونقلها و أن تقنيات معالجة المعلومات تتضمن ثلاثة محاور رئيسة هي :

1- انتشار محطات العمل أو الحاسب الآلي الكبير .
2- ظهور الحاسب الشخصي .
3- شبكات الحاسب الآلي .

حيث أن شبكات الحاسب الآلي شكلت قفزة نوعية في مجال جمع المعلومات وتوزيعها وأصبح الحاسب الآلي وعمليات الاتصالات الأداتين الرئيستين لتقنية المعلومات ونتج من دمجهما معاً الأداة القوية في التعامل مع تقنية المعلومات عن طريق شبكة الإنترنت .

فلم يعد الحاسب الآلي اليوم محصوراً في قدرته على تخزين كم هائل من المعلومات ولا بقدرته على تصنيفها وتنظيمها أو سرعة استرجاعها ، وإنما وقبل ذلك كله ، قدرته على الاتصال بمصادر المعلومات الأخرى والتفاعل معها ولا سيما في إرسال المعلومات واستقبالها.

ومع إطلالة القرن الحادي والعشرين أصبح من الصعوبة الاستغناء عن أجهزة الحاسب الآلي في مواكبة التطورات الحديثة في جميع مجالات الحياة ، حيث أنه لا يوجد مجال من مجالات الحياة لم يدخله الحاسب الآلي كما أشار سلامة (1996) و مهدي علي (1998) إلى :

1- السرعة العالية في المعالجة والحصول على النتائج (أي سرعة تنفيذ ملايين العمليات)
2- الدقة العالية (أي دقة الحصول على نتائج دقيقة) .
3- الوثوقية (أي إمكانية الحاسب الآلي للعمل بصورة متواصلة ولفترات طويلة دون كلل أو ملل والحصول على نتائج صحيحة) .

4- إمكانية هائلة في التخزين (أي تخزين كميات هائلة من البيانات والمعلومات والحصول عليها بالسرعة الفائقة عند طلبها من الجهاز في وقت يشاء) .

5- تنسيق النصوص وعمل الرسوم بألوان دقيقة وجذابة وتحريكها وتسجيل الأصوات وإذاعتها وتبادل المخاطبة مع مستخدمها بواسطة النصوص المقروءة على الشاشة أو المسموعة من خلال أجهزة مرتبطة بالحاسب الآلي مع إمكانية عرض الفيديو) .

6- إجراء الاتصالات (أي إمكانية الاتصال مع أجهزة الحاسب الآلي في جميع دول العالم من خلال شبكة العالمية ، ومراكز المعلومات في دول العالم لتشمل على النصوص المقروءة والوسائط المتعددة التي تتضمن الرسوم والصور والأشكال والأصوات والفيديو وغيرها .

ومن خلال ما سبق فإن الباحث يعرف الحاسب الآلي بأنه جهاز إلكتروني يعمل وفق برنامج مخزون ، حيث يستقبل المدخلات ويعالجها وفق قواعد محددة ويعطي نتائج تسمى مخرجات وبمعنى آخر هو عبارة عن جهاز معالج للمعلومات وليس لحل المسائل الحسابية وحسب ، كما أن الحاسب يملك سرعة خارقة في تنفيذ الأوامر الموكلة إليه ، إذ يقوم بإجراء ملايين العمليات بسهولة كبيرة ووقت زمني قصير .

المحور الأول: حجم الخسائر المادية الناجمة عن الجريمة المعلوما تية

إن لم تكن الجرائم المعلوماتية معرفة بشكل كبير فإنها بدأت تتسم ببعض المرونة و السرعة و التهكير الناعم و الصامت و العابر للحدود خاصة الجرائم التي تستهدف المؤسسات الإستراتيجية، لذلك وجب علينا التعريج على ماجاء به المشرع الجزائري من خلال تعريفاته للجريمة المعلوماتية و كذا انواع الفيروسات لتهكير و قرصنة الانظمة المعلوماتية.

إن تحول الاقتصاد العالمي من مرحلة الاقتصاد التقليدي إلى مرحت الاقتصاد الرقمي وتحول التعاملات التجارية والمالية إلى شكل الكتروني زاد من خطورة الجريمة الإلكترونية والتي أصبحت في تصاعد مستمر ومن المتوقع أن يتزايد حجم الخسائر التي يتكبدها العالم بسبب الجريمة الإلكترونية في العقود القليلة المقبلة ' نتيجة تزايد عدد الشريكات التي تعتمد على الأنترنت في ممارسة نشاطاتها.[1]

وقد أشارة توقعات أن الجرائم الإلكترونية قد تتسبب بخسارة دول المجلس الخليجي بين 550 مليون و735 مليون دولار أمريكي سنويا' كما أكد اقتصادي متخصص أن معدل نسبة الجرائم الإلكترونية في العالم يصل إلى 57,6% حيث يكلف الاقتصاد العالمي ما يقارب 12,950 مليار دولار سنويا [2]

ـ ووفقا لتقرير صادر عام 2013م عن معهد المحاسبة العامة cpas في الولايا المتحدة الأمريكية , كانت الخسائر التي لحقت الشركة التجارية نتيجة للجرائم المعلوماتية بإجمالي مبلغ 7,2 مليار دولار عام2010م, وقد ذكر التقرير قائمة بأعلى الجرائم المعلوماتية الأكثر ارتكبا , وهي خمسة أنواع من السرقات المعلوماتية وهي على النحو التالي:1) ـ سرقة المبالغ المعادة من الضرائب . 2) ـ سرقة البيانات الشخصية. 3) ـ سرقة الممتلكات والمنتجات الفكرية

ـ وفي تقرير أصدره بنك في أمستردام انه تم تحويل مبلغ 8,4 مليون دولار الى بنك في سويسرا من قبل شاب يبلغ من العمر 26 سنة ٬ وفي عام 2000 م جر السطو على 33 ألف جهاز صرف آلي ATM في بريطانيا , وقد كانت الخسائر المالية كبيرة قدرت ب 15مليون إسترليني.[182]

ـ كما ورد في التقرير السنوي الثامن لمكتب التحقيقات الفدرالي الأمريكي الصادر عام2003[183] بعنوان جرائم الحاسب بأن خسائر المؤسسات بولايات المتحدة الأمريكية [184] أتى من استيلاء على المعلومات و التى كبدتها خلال هذا العام خسائر تتعدى 70 مليون دولار أمريكي وبأتي في المركز الثاني نشاط تعطيل نظم المعومات محققا خسائر تتجاوز 65,5 مليون دولار.[3]

أولا: موقف المشرع الجزائري من الجريمة المعلوماتية

على خلاف المشرع الفرنسي الذي لم يعط تعريفا للجريمة المعلوماتية فإن المشرع الجزائري قد اصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال، وعرفها بموجب المادة الثانية من القانون 04-09 على أنها "جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أية جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.

يمكن استنتاج النقاط التالية من خلال هذا التعريف:

---

[182] زيبحة زيدان , الجريمة المعلوماتية في التشريع الجزائري والدولي, دار الهدى للطباعة والنشر والتوزيع , مليلة الجزائر .2011, ص 11 ,

[183] أنظر مقال بشأن تأثير الجريمة المعلوماتية على النواحي الإقتصادية, http// kenanaonline .com/ ahmedkordy, اطلع علية 07/15 /2020 .

[184] أحمد محمد عبد الرؤف المنفي , السرقة الإلكترونية وحكمها في الإسلام, الطبعة الثانية , E_Kutub Ltd , شركة في بريطانيا مسجلة في انجلترا برقم 7513024 , لندن , يونيو 2018 , ص13ـ 14

1:أن المشرع الجزائري قد اعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الالكترونية أولها معيار وسيلة الجريمة وهو نظام الاتصالات الالكتروني، و ثانيها معيار موضوع الجريمة المساس بأنظمة المعالجة الآلية للمعطيات، وثالثهما معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.

2: كما اعتمد المشرع الجزائري على معيار رابع في تحديد نطاق الجريمة الالكترونية، كونه أقر أن الجريمة الالكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، و هذا ما يوسع من نطاق مجال الجرائم الالكترونية في القانون الجزائري[185].

وترتيبا على كل هذه التعاريف الفقهية و التشريعية، يمكننا تعريف الجريمةالمعلوماتية بأنها "كل سلوك غير مشروع يمس بالنظام المعلوماتي المادي أو المعنوي " أو كل سلوك غير مشروع يقع على النظام المعلوماتي أو بواسطته ويمس بالأشخاص أو الأموال أو أمن الدولة. أي أن الجريمة المعلوماتية على سبيل الجرائم التقليدية تعرف من خلال أركانها أي توفر القصد الجنائي لارتكاب هذه الجريمة و الركن المادي للجريمة و ركنها القانوني.

في ضل شيوع شبكات المعلومات وفي ظل التوسع والنماء الكبير لأنظمة الحواسب المفتوحة ونقل وتدفق المعلومات ، إضافة إلى التشديد على أهمية مكافحة كافة الأنشطة التي تستهدف العناصر الثلاثة لأمن المعلومات ونظم الكمبيوتر وهي السرية وسلامة المحتوى ، و توفر المعلومات برزت على المستوي الإقليمي عدة جهود لمكافحة هذا النوع من الجرائم

من أهمها جهود المجلس الأوربي الذي يحاول تكريس وجوب التعاون بين أعضاء الإتحاد لمواجهة هذا النمط المستحدث من الإجرام سواء فيما بينهم أو بالتنسيق مع هيئات ومنظمات دولية أخرى، ففي عام 1981 تم التوقيع على اتفاقية الخاصة بحماية الأفراد من إساءة استخدام البيانات المعالجة الكترونيا، وذلك من خلال إقراره العديد من التوصيات الخاصة لحماية البيانات ذات الصبغة الشخصية من سوء الاستخدام وحماية تدافق المعلومات[186]

---

[185]نمديلي رحيمة، خصوصية الجريمة الالكترونية في القانون الجزائري و القوانين المقارنة، أعمال المؤتمر الدولي الرابع عشر: الجرائم الالكترونية، طرابلس 24-25 مارس 2017، ص95.

[186] صراع كريمة, دقيش جمال ,الأبعاد الإقتصادية للجريمة الإلكترونية , مجلة الدراسات التسويقية وادارة الأعمال, المجلد02, اعدد01, جانفي2018 , ص47/48

ـ في عام 1992 وأثناء الحملة الإنتخابية للرئيس الأمريكي "بيل كلينتون" حيث اعلن انه يعد أن يجعل من طريق المعلومات السريع حجر زاوية جديد في البنية الأساسية القومية يشابه في أهميته نظام الطرق السريعة بين أرجاء الولايات المتحدة الأمريكية أي أنه يعد أحد المرافق الأساسية العامة , وبذلك انتقلت الفكرة الى المجال الإداري ليمنح الآلة الحكومية الضخمة فرصا للتغير من خلا ل أساليب عمليها وخدمة عملائها الجماهير العريضة, تم أخذت دول أروبية عديدة بتطبيق نظام الحكومة الإلكترونية مثل هولنداا و كندا .

3ـ وقد تضمن تلك الإتفاقية عدة مبادئ تمثلت في الحد الأدنى من الإحتياطات التى يجب أ، تتضمنها التشريعات الداخلية لدول أطراف , المعاهدة لحماية الأفراد من اساءة استخدام البيانات المعالجة الكترونيا, وضرورة الحصول على البيانات الشخصية من مصادر مشروعة , وأن تكون البيانات صحيحة ومتفق مع الغض الذي وضعت من أجله , و أن تكون المعلومات حديثة , وأن تراعى القواعد الشكلية اللازم اتباعها للحيلولة دون اساءة استخدام البيانات الشخصية .

-وقد تم كذلك بنشر دراسة تضمنت توصيات تفعيل دور القانون لمواجهة الأفعال الغير مشروعة عبر الحاسب سنة1989 وهي التوصيات التي لحقتها دراسات أخرى [1] ، منها التوصية رقم 13195في سبتمبر 1995 م في شأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات وذلك تحث الدول الأعضاء لمواجهة القوانين الجنائية الوطنية لتلائم التطور في هذا المجال [2].

ثانيا: التقنيات المستخدمة في تدمير النظام المعلوماتي:

المقصود بالتقنيات هي التي من شأنها إتلاف أو محو تعليمات البرامج أو البيانات التي يتم معالجتها آليا والهدف من وراء التدمير ينجر من وراءه تحقيق منافع شخصية سواء الاستيلاء على النقود أو مجرد الاطلاع عبر شبكة الأنترنيت وقد تصل الرغبة أحيانا إلى إصابة الحاسب الآلي بالشلل التام وإعاقته عن القيام بأداء وظائفه الطبيعية، هناك عدة وسائل وطرق لتدمير النظام المعلوماتي:

*.الفيروسات: يمكن تعريف الفيروسات على أنها مجموعة من العمليات التي تتكاثر بمعدل سريع وتصيب النظام المعلوماتي بشلل تام، هناك عدة تعريفات للفيروس منها:

*عبارة عن خلية مغناطيسية نائمة ومبرمجة، تنشط في وقت محدد لتخريب البرنامج الأصلي ومنتشرة في الأجهزة الأخرى التي تضمها الشبك بحيث تفسر ما تحويه من معلومات(محمد س.، 1993، صفحة 45)البعض الأخر يعرفه على أنه " برنامج يصممه بعض المختصين بهدف تخريبي مع إعطاءه القدرة على ربط نفسه ببرامج أخرى ثم يتكاثر وينتشر داخل النظام حتى يتسبب في تدميره تماما.

من بين خصائص الفيروسات، أنها تضع من طرف فئة مريضة من خبراء البرامج، أما لإثبات الذات أو مجرد الدعاية، أو إلحاق الضرر والأذى، فهاته الفيروسات تتمتع بقدرة فائقة في مهاجمة البرامج وأجهزة الحاسبات، المعطيات، البيانات، والمعلومات وكأن الفيروس الحاسوبي يتشابه مع الفيروس العضوي(فيروس في اللغة اللاتينية، "سم" عرف هذا المصطلح في مادة العلوم البيولوجية) من حيث عدم جدواه إلا أن الأول يمكن له أن ينتشر عبر الشبكات ويعبر الدول والقارات وهذه سمة أساسية للجرائم المعلوماتية.

*.أنواع الفيروسات: هناك عدة تسميات لهاته الفيروسات أهمها:

- بوت سكتور"boot sector" يصيب هذا الفيروس جزء من قسم البرنامج، الذي يحتوي على نظام التشغيل والملفات والمعلومات ويتميز بالإنتشار السريع.
- -فايل "file": يصيب هذا الفيروس ملفات Eve، com، ثم يقوم بنسخ نفسه كلما جرى تشغيل البرنامج المصاب.
- فيروس حصان طروادة : هذا الفيروس بالذات حصل نصرا عسكريا وأسطوريا(إبراهيم ، 1949، صفحة 125)فيالعصور الوسطى هاته الأخيرة، تمكنت من إختراق أجهزة الحاسبات في أرع دول أوروبية هي إنجلترا، السويد الدانمارك، النرويج.
- فيروس الكريسماس: يظهر هذا الفيروس في شكل رسالة بريدية إلكترونية تعرض فيها بطاقة تهنئة للكريسماس على شاشة الحاسب الآلي ومما يترتب عن قبول التهنئة، توقف النظام كليا[187].

المحور الثاني: الحماية الجزائية للنظام ألمعلوماتي:

إن قضية الأمن ألمعلوماتي أصبحت تشغل الكثير من الدول ، لأهميته الأمني ولاستقرار البلدان على برامج معلوماتية ذات ثقة وجودة عالية. يتسع مفهوم أمن المعلومات ليشمل الإجراءات والتدابير المستخدمة في المجالين الإداري والفني لحماية المصادر البيانية من أجهزة وبرمجيات وبيانات وأفراد، من التجاوزات والتداخلات غير المشروعة(نادر عبدالكريم ، 2009، صفحة 25)التي تقع عن طريق الصنعة أو عمدا عن طريق التسلل أو نتيجة لإجراءات خاطئة أو غير الواقعية المستخدمة من إدارة هذه المصادر فالأمن المعلوماتي يمكن عرقلته عن طريق الخطوات التالية:

---

[187] صيقع سيد أحمد , الإطار القانوني للجريمة المعلوماتية في القانون الجنائي الجزائري وطرق مكافحتها , مذكرة لنيل شهادة الليسانس , جامعة ابن خلدون ـ تيارت , كلية الحقوق والعلوم السياسية , قسم العلوم القانونية والإدارية , 2007/2006 ,ص39 .

- الأخطاء العفوية غير المتعمدة أثناء تجهيز البيانات لإداخلها على الحاسبة.
- حوادث فقدان أو تغير المعلومات بسبب تعطيل الأجهزة أو حصول خلل في البرامج.

-سرقة المعلومات أو التقاطها وتغييرها بشكل غير مأذون وما ينتج عن هذا من سوء استخدام هذه المصادر

أولا: الجزاءات المقررة للاعتداءات الماسة بأنظمة المعالجة للمعطيات

طبقا لأحكام المادة الأولى من الاتفاقية الدولية في الجرائم لمعلوماتية التي صادقت عليها الجزائر، إن العقوبات يجب أن تكون رادعة وهذا ما انتهجه المشرع الجزائري في تحديد هذه العقوبات المطبقة على الشخص الطبيعي والمعنوي نذكر من خلالها ما يلي :

أ ـ العقوبات الأصلية

إذ نجد هناك تدرج للعقوبات المقررة في الشخص الطبيعي في حالة جريمة الدخول أو البقاء الغير مشروع في صورتها البسيطة , وفي الدرجة الثانية عقوبة مقررة لنفس الجريمة المشددة ، وفي الدرجة الثالثة عقوبة مقرر للجريمة الخاصة بالمساس العمدي للمعطيات ، وهي عقوبات يجمع فيها احبس والغرامات حسب الدرجات

ب ـ العقوبات التكملية وتتمثل في :

ـ المصادرة التي يمكن أن تنصب على الأجهزة والبرامج والوسائل المستعملة في ارتكاب جريمة من هذه الجرائم

ـ إغلاق المواقع التي تكون محل للجريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

ـ إغلاق المحل أو المكان الاستغلال الذي ارتكبي على مستواه الجريمة شريطة علم المالك

ج ـ حالات الشخص المعنوي

تجدر الإشارة أن الشخص المعنوي يسأل عن هذه الجريمة بصفته فاعل أصلي أو شريك بشرط أن يرتكب الجريمة بواسطة أحد أعضائه أو ممثله مع العلم أن المسؤولية الجزائية للشخص المعنوي لا تتحقق دون قيام مسؤولية الأشخاص الطبيين بصفة الفاعلين في الجريمة [188] لم يقف العالم موقف المتفرج حيال سرعة تطور الجريمة المعلوماتية اذ لامس خطورتها منذ البداية

---

[188] ـ بن دعاس فيصل , اشكالات الجريمة المعلوماتية في التشريع الجزائري, محاضرة في اطار التكوين المحلي المستمر للقضاء, مجلس قضاء قسنطينة، 2011/2010 , ص 13 .

2 ـ نصت عليها المادة 12 من الاتفاقية الدولية الأجرام المعلوماتي الجهود الدولية في مجال مكافحة الجريمة المعلوماتية

حيث أصبح هذا النوع من الجرائم يعبر الحدود ليلحق الضرر بعدة دول ومجمعات ولم يعد يتمركز في دولة معينة ولا يوجه لمجتمع بعينه نتيجة التطور الكبير لوسائل التقنية الحديثة في الاتصالات ودخول جميع فئات المجتمع إلى قائمة مستخدميها، فل يتردد المنحرفون منهم في استغلالها لأغراض دنيئة[2] ومن أجل ذلك كان من الضروري أن تتضافر جهود الدول سواء على المستوى الداخلي أو الخارجي لمواجهتها ، وذلك من خلال إصدار القوانين وإبرام اتفاقيات بهذا الخصوص وعليه فان هذا المطلب يتناول بالدراسة على أربع فروع هي[189]:

- أهم الا تفاقيات الدولية في مكافحة الجريمة المعلوماتية
- جهود الأمم المتحدة من خلا منظمة اليونسكو كمنظمة تابع لها
- الجهود المبذولة على المستوى الإقليمي
- الجهود المبذولة على المستوى الوطني

ثانيا: أهم الاتفاقيات الدولية في مكافحة الجريمة المعلوماتية

إن من باب التذكير بالمجهود الدولي في مجابهة الإجرام الإلكتروني ين القول بأن بعض الاتفاقيات الدولية لا تزال تتخذ كمرجع لصياغة النصوص المتعلقة بوضع الإطار القانوني لحماية النظام المعلوماتي بشكل عام والتجارة الإلكترونية ومنها الاتفاقية المتعلق بالتجارة GATT,الاتفاقية العامة لتعويضات والتجارة. والتي تم إقرارها في 1947/10/30 بعد الحرب العالمية الثانية.ونتيجة لما لمسه الحلفاء من كساد اقتصادي وقد تم التوقيع النهائي على الوثيقة الختامية المتضمنة لنتائج جولة أورقواي للمفاوضات التجارية المتعدد الأطراف والتي خلصت إلى إنشاء منظمة التجارة العالمية WTO والتي ألحقت بيها فيما بعد اتفاقيات أ خرى ومنها الخاصة بالحقوق الملكية لفكرية والمعروفة باتفاقية التربيس ـ اتفاقية أوجه التجارة المتعلقة بالملكية الفكرية في73 مادة , وهنالك اتفاقية برن في : 1886/09/09 الخاصة بحقوق المؤلف والتي خضعت إلى عدة تعديلات كان أخرها تعديل باريس في: 1971/07/24 و1979/09/28 وقد انضمت إليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم:34/97 في1997/09/13 ويندرج في مضمار ذلك اتفاقية باريس الخاصة بحقوق الملكية الصناعية والتي أبرمت في : 1883/04/20[190]

---

[189] صراع كريمة .دقيش جمال, الأبعاد القانونية للجريمة الإلكترونية,مجلة الدرسات التسويقية وادارة الأعمال , المجلد02 العدد 01 , جانفي 2018 ص47 .

[190] سيد طنطاوي محمد سيد , الجريمة المعلوماتية" الصعوبات التي تواجه التعاون الوطني والدولي وكيفية مكافحتها ", مجلة المركز الدمقراطي العربي للدراسات الإستراتيجية والإقتصادي والسياسية , 2018/01/17, ص 15 .

ويبدو أن اتفاقية القات g.a .t.t لتحرير التجارة والتي تولدت عنها منظمة التجارة العالمية كما أسلفنا وكذا الاتفاقية الخاصة بحقوق الملكية الفكرية المسماة trips تضلان من أهم الأطر القانونية القائمة كآلية دولية لفرض الحماية القانونية المطلوبة والتي ضلت تدفع في اتجاه خلق ضوابط أخرا إذ تجدر الإشارة إلى معاهدة جنيف الخاصة بقانون العلامات التجارية ولائحات التنفيذية والتي ابرزتها الى جهود المنظمة العالمية للملكية الفكرية wipo, ومن المعلوم أنها تمتلك مركز متخصص في تسوية المنازعات المتعلقة بالملكية الفكرية والتي تطرأ بين الأفراد والشركات ومما يجب التنويه بيه هنا أن هيئة الأنترنت المتخصصة بأسماء والأرقام أو ما يعرف بالحقل أو الدومينDOMEN أعمدت هذا للتصدي للقضايا والنزاعات المثارة.

ومعلوم أن الحقل أو الدومين يؤدي وضيفة مثل دليل الهاتف يحدد الموقع الإلكتروني لشخص مامستخدم لجهاز الحاسوب ويتم تبادل المعلومات معه دون الاختلاط مع صاحب الموقع الأخر غير أن ، اللافت للانتباه أن هذا الموقع أصبح يصطلح عليه بالإرهاب الإلكتروني .[1]

الفرع الثاني : جهود الآمم المتحدة من خلا منظمة اليونسكو كمنظمة تابع لها

تتعتبر الأمم المتحدة هيئة ذات إرادة مستقلة, تتمتع لا شخصية قانونية دولية قائمة على أساس اتفاق بين مجمعة من الدول ذات السيادة وتعتبر العضوية فيها مفتوحة لكل دولة تتمتع بالسيادة ويبلغ عدد الدول الأعضاء فيها 192 دولة[191] ولعل من مبادئها و أهدفها نجد المساواة بين الدول في السيادة , وحفظ الأمن والسلم الدوليين .

اكدت جهود أمم لمتحدة في مكافحة أو منع الجريمة معاملة المجرمين المتعلق بجرائم التقنية أو جرائم المعلوماتية، حيث عملت هذه الأخيرة منذ نشأتها على رسم سياسة ناجعة في مجال منع الجريمة وتحقيق عدالة الجنائية ، عبر إقرار العديد من التوصيات لعل من أبرزها التوصيات الأمية بشأن مجتمع المعلوماتي

مما أنشاء اللجنة المتخصصة مثل اللجنة الاستشارية لخبراء من الجريمة ومعاملة المجرمين، الذي عهد إليها مهمة مكافحة الجريمة وتقديم المنشورة للأمين العام ، و إيجاد البرامج ووضع الخطط ، ورسم سياسات لتدابير دولية في مجال مكافة الجريمة ، وهي تعقد مؤتمرات دولية كل05 سنوات ن أجل تعزيز التبادل بين مختلف الدول من أجل تدعيم التعاون الدولي والإقليمي في هذا المجال , ومن بين هذه المؤتمرات نجد مؤتمر

---

[191] **أنظر مقال بعنوان الجهود الدولية في مجال مكافحة جرائم الأنترنت .http://www. Startimes .com , اطلع عليه بتاريخ 2020/07/16.**

الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين والذي تم انعقاده في مدينة ميلانو بايطاليا سنة 1985م ،والذي انبثق عنه من القوعد التوجهية والتي توجت بالمصادقة على هذه المبادئ في هافانا بكوبا عام1990م فقد أكد هذا الأخير على ضرورة الاستفادة من التطورات العلمية والتكنولوجيا في جرائم الحاسب آلي , كما أكدا على ضرورة اعتماد ضمانات لصون سرية البيانات الشخصية المخزنة في الحاسب آلي وأهم مبادئ مؤتمر هافانا (1990م):

- &-تحديث القوانين الجنائية الوطنية بما في ذلك التدابير المؤسساتية .
- &-تحسين أمن الحاسب الآلي والتدابير الفنية .
- &اعتماد إجراءات تدريب كافية للموظفين والوكالات المسؤولية عن منع الجريمة الاقتصادية والجرائم المتعلقة بالحاسب الآلي والتحري والإدعاء فيها.
- &-تلقين آداب الحاسب الآلي كجزء من مفردات مقررات الاتصالات والمعلومات.
- &-اعتماد سياسات تعالج الاشكالات المتعلقة بالمجني عليهم في تلك الجرائم[2]

ويبدو أن جهود الأمم المتحدة لم تقف فقط في هذا المجل بل عقدة العديد من الاتفاقيات غفي سبيل مكافحة كل أنواع الجرائم والجريمة المستحدثة و فقد عقدة اتفاقية خاصة سنة 2000لمكافحة إساءة استخدام تكنولوجيا المعلومات لإغراض إجرامية ، وعقب ذلك عقد مؤتمر بالبرازيل في أفريل سنة 2010 م بحيث تناولت أعمال تحليل الظاهرة وإحصائيات المتعلقة بالجريمة الإلكترونية[192] ،

إجراءات التحقيق، الأدلة الإلكترونية ، المساعدة التقنية الدولية، خدمات الأنترنت، التعاون الدولي للتصدي للجريمة الإلكترونية ، بإضافة إلى أعمال الجنة الاقتصادية و الاجتماعية لغربي أسيا التابعة للمجلس الاقتصادي و الاجتماعي تحت غطاء منظمة الأم المتحدة سنة2008م ، ومن ثم أفريل 2015م[193]

---

[192] معوان مصطفى , الإثبات في المعاملات الإلكترونية في التشريعات الدولية "التوقيعات والتوصيات الإلكترونية " , الطبعة01, منشورات دار الكتاب الحديث، القاهرة ,2008، ص 147/112 .

[193] ـأنظر مقال بعنوان الجهود الدولية في مجال مكافحة جرائم الأنترنت .http://www. Startimes .com , اطلع عليه بتاريخ 2020/07/16.وقد جاء ت جهود الإسكوا ESCWA الرامية إلي تطوير التشريعات الإلكترونية ومواءمتها ،وكذا إنشاء مجتمع المعرفة في المنظمة العربية ، مع التركيز على الأطر التنظيمية والإجرامية لمكافحة الجريمة الإلكترونية وظمان سلامته، وتجدر بنا الإشارة أن الولايات المتحدة الأمريكية هي أول من ندى بإنشاء الحكومة الألكترونية ففي عام 1981 تم التوقيع على اتفاقية الخاصة بحماية الأفراد من إساءة استخدام البيانات المعالجة الكترونيا

إن أهم ما ورد في توصية المجلس الأوروبي هو :-

- أن توضح القوانين إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات التي تحويها المعلومات أثناء انتقالها.
- أن تسمح الإجراءات الجنائية لجهة التفتيش بضبط برامج الكمبيوتر و المعلومات الموجودة بالأجهزة وفقاً لذات الشروط الخاصة بالتفتيش العادي[194].
- تطبق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي في حالة الضرورة في مجال تكنولوجيا المعلومات.
- يجب إلزام العاملين بالمؤسسات الحكومية والخاصة التي توفر خدمات الاتصال بالتعاون مع سلطات التحقيق لإجراء المراقبة والتسجيل.
- يتعين تعديل القوانين الإجرائية بإصدار أوامر لمن يحوز معلومات (برامج – بيانات) تتعلق بأجهزة الكمبيوتر وتسليمها.
- يجب أن تكون هناك إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة[195]. يتعين عندئذ أن تسمح السلطة الأخيرة بإجراء التفتيش والضبط
- ولعل من أهم ما قام به المجلس الأوروبي هو وضع اتفاقيت بودابيست الصادرة في 2001/11/23 حيث تشكل نصوصها منظومة تعاون دولي تتسم با لمرونة الفعالية وتعمل على إحداث تقارب التشريعات الجنائية الخصة بهذه الجرائم وتكفل استخدام الوسائل الفعالة في البحث والتحقق وملاحقة مرتكبيها .[1]

والتي وقعت عليها 26 دولة من أعضاء الإتحاد الأوروبي إضافة إلى كندا واليابان, وجنوب إفريقيا ، والولايات المتحدة الأمريكية، وأستراليا ، نتاج مفوضات استغرقت ـكثر من أعوام حتى تم التوصل إلى الصيغة النهائية المناسبة لهذه الاتفاقية [2]

وقد تضمن هذه الاتفاقية 48 مادة غطت في مضمونها ثلاثة أقسام كبرى:

---

[194] فهد دحين العدواني , الأنترنت والجريمة الإلكترونية وطرق التغلب عليها , مجلة الدولية للتعليم بالأنترنت ، دسمبر , 2016 , ص 73.

[195] سعيداني نعيم , آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري, مذكرة لنيل الماجيستير في العلوم القانونية, جامعة الحاج لخضر ـ باتنة, كلية الحقوق والعلوم السياسية , قسم حقوق ,2013/2012 , ص85 .

ـ القسم الأول : تناول مجموعة الجرائم التي يمكن أن تتعرض لها النظم المعلوماتية

ـ القسم الثاني : تناول مجموعة الإجراءات الجنائية التي يمكن أن تتحد في مواجهة هذا النوع من الجرائم خصوصا تفتيش وضبط البيانات الخزنة في الحاسوب

ـ القسم الثالث : تناول موضوع التعاون الدولي بين الدول الأعضاء الموقع على الاتفاقية.[3]

وعلاوة علا ذلك اعتمد الإتحاد الأوروبي في عام 2003 إطار قانونيا بشأن نظام المعلومات والتي دخلت حيز التنفيذ في سنة 2005.[4]

الخاتمة

ـي ختام هذه الدراسة الخاصة بالجريمة الإلكترونية استخلصنا أن هذه الجريمة تختلف من حيث طبيعتها و تعريفها عن باقي الجرائم التي عهدناها بالإضافة إلى صعوبة وضع تعريف جامع و موحد لها و ذلك مما أدى إلى اختلاف المفاهيم و تعاريف حولها فهناك من عرفها على أساس وسيلة ارتكاب الجريمة و هناك من عرفها على أساس محل أو موضوع الجريمة، و البعض الآخر على أساس شخصية الجاني، و الآخر جمع بين عدة تعاريف.

كما أن طبيعتها الخاصة تجسدت في خصائصها المتميزة و المتمثلة في أنها جريمة عابرة للحدود و لكونها ترتكب بواسطة الحاسوب و في مجال الحاسب الآلي، كما أنها تتميز بالسرعة في التنفيذ و يغلب عليها التطور المستمر و متسارع من حيث ارتكابها و إلى جانب هذا هناك الخصوصية التي يتميز بها المجرم المعلوماتي و صفاته، باعتباره لا يلجأ إلى العنف كما هو الحال في المجرم التقليدي، بل يتميز بالذكاء و المهارة و المعرفة و هذا ما جعل القوانين الحالية عاجزة عن مكافحة هذا النوع من الجرائم نظرا للتطور الحاصل بمجال تقنية المعلومات، إلا أنه نجد في المقابل الهيئة التشريعية الجزائرية تحاول جاهدة مواكبة هذا التطور الإجرامي و مكافحته من خلال العديد من الإجراءات المنصوص عليها في القانون العام ونقصد بذلك قانون الإجراءات الجزائية و قانون العقوبات الجزائري أو في قوانين و هياكل خاصة منها القانون رقم 09-04 و الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال.

و في الأخير يمكن القول أن المشرع الجزائري أحدث سبل قانونية للتصدي لهذه الجرائم الخطيرة و تماشيا مع النظام العالمي الدولي المبني على التطور التكنولوجي و السرعة في الاتصال و يهدف ذلك لتطوير

منظومته القضائية للتصدي لهذه الجريمة، ما تبقى سوى تفعيل حقيقي و مادي للنصوص القانونية و تكوين متخصصين في مجال الإلكتروني بشكل جدي الذين يقومون بالتحري و التحقيق و اكتساب مهارات الدول التي قطعت شوطا في مكافحة هذه الجريمة.

و من خلال ما سبق نقدم الاقتراحات التالية:

1. رسم استراتيجية متكاملة للأمن الإلكتروني و مكافحة الجرائم الإلكترونية باشراك جميع القطاعات الحكومية، و خاصة المعنية، و توفير التغطية التقنية و المالية لتنفيذها.

2. سد الفراغ التشريعي في مجالات البيئة الرقمية بتشعباتها كافة مع إصدار المذكرات التوضيحية للتشريعات، لاسيما في مجال مكافحة الجريمة الإلكترونية، على أن يكون شاملا للقواعد الموضوعية و الإجرائية، مع الحرص على أن تكون هذه التشريعات منبثقة من المجتمع المحلي و عدم استيرادها جاهزة حرصا فعاليتها.

3. إنشاء هياكل متخصصة في مكافحة هذا النوع من الإجرام المستحدث، و هذا ما تم تجسيده و العمل به من قبل المشرع الجزائري كإنشاء الهيئة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال...إلخ، لكن هذا لا يزال يحتاج لتفعيل حقيقي لعمل الهيئة و المراكز المتخصصة الأخرى و إعطائها كامل الحرية و الاستقلالية في إنجاز مهامها بشرط عدم تعارض ذلك مع الحريات الخاصة...إلخ، و حبذا لو تم وضع هذه الهيئات تحت يد القضاء الذي يستطيع أن يوازن بين المصالح العامة و الخاصة...

4. تشجيع على خدمة تلقي الشكاوى و البلاغات إلكترونيا و العمل بها و نشر ثقافتها... من خلال تحسيس الأشخاص بصفة عامة و الضحايا بصفة خاصة على التبليغ على مثل هذه الجرائم بسرعة من أجل ضمان سهولة الكشف عن الجريمة الإلكترونية و سرعة اتخاذ الإجراءات بشأنها.

5. العمل على إعادة النظر في المناهج الدراسية في كليات القانون، و ضرورة تضمينها مادة عامة عن الحاسب الآلي و الشبكات المعلوماتية، بالإضافة إلى ضرورة إدراج الجانب المعلوماتي لكل مادة قانونية.

6. تعزيز المساعدة الفنية لمختلف هيئات العدالة، و أجهزة النيابة العامة و السلطات القضائية في مجال منع الجريمة المعلوماتية و مكافحتها، و تأمين الوسائل التقنية و المكننة اللازمتين لذلك.

7. إنشاء جهاز خاص داخل الشرطة يختص بالبحث و التحري عن هذا النوع من الجرائم و وضع سياسة تكوينية و تدريبية تتماشى و التطورات التكنولوجية الهائلة.

8. ضرورة تكثيف الجهود الوطنية لنشر المعرفة و زيادة الوعي بالجرائم الإلكترونية و مدى خطورتها و وسائل الوقاية منها و سبل مواجهتها.

9. ضرورة إيجاد الوسائل المناسبة للتعاون الدولي لمكافحة هذه الجريمة من الناحية الإجرائية بهدف التوفيق بين التشريعات الخاصة بهذه الجرائم كالتعاون الدولي على تبادل المعلومات و تسليم المجرمين و قبوا أي دولة للأدلة المجوعة في دول أخرى لضمان الحماية العالمية الفعالة لبرامج المعطيات الآلية و الكمبيوتر و شبكة الأنترنت ككل.

10. ضرورة إبرام اتفاقيات عربية و دولية في مجال مكافحة الجرائم الإلكترونية، و ذلك لتحديد إطار الاختصاص القضائي الدولي و التعاون في كشف و إثبات الجريمة الإلكترونية.

-إن الدول العربية مستهدفه بشكل كبير بحكم الالتزام بتعاليم الشريعة الإسلامية ، وبحكم موقعها الجغرافي ، وبحكم مالديها من ثروات طبيعية وبشرية ، لذلك لأبُد من التفكير والتلاحم في مستقبلنا المعلوماتي والتكنولوجي.

وإذا كانت الدول المتقدمة علمياً تراهن على طلابها الجامعيين في صناعة مستقبلها والحفاظ على تقدمها، فإن الدول العربية لذلك أحوج .

الحرب السيبرانية من منظور القانون الدولي

الدكتور نايف أحمد ضاحي
أستاذ القانون الدولي العام في كلية الحقوق جامعة تكريت (العراق)

الملخص:

شهد المجال الحربي طفرة كبيرة مع التحول التكنولوجي والرقمي الذي يعيشه العالم اليوم، إذ تطورت وسائل الحروب بفضل هذا التحول في جزء مهم منها من معارك مباشرة، إلى أخرى تدار من خلال عالم افتراضي إلكتروني، قد تتجاوز خطورته الأشكال السابقة للحرب.

ووفقا لذلك، باتت الحرب الإلكترونية والسيبرانية، تمثل أنواعا جديدة من الأسلحة في العصر الحالي، قادرة على إحداث أضرار جسيمة وواسعة النطاق للبنية التحتية الحيوية لدولة ما، وتمثل وجها آخر للقوة قد تلجأ إليها الدول في معاركها، بعد أن خضعت الوسائل التقليدية لاستعمال القوة إلى التغيير، بفضل التطورات الحاصلة. الأمر الذي يتطلب من المجتمع الدولي التوصل إلى بعض الإجماع حول معنى الحرب السيبرانية، وإلى اتفاق دولي يحكمها.

في هذه الورقة التحليلية، سنبحث في مسألة ما إذا كان يمكن اعتبار الهجمات السيبرانية، ترقى إلى المستوى الحقيقي للحرب، ومشروعية اللجوء إليها في إطار القانون الدولي فيما يتعلق بحق استخدام القوة في إطار القواعد القانونية المؤطـــرة لهذا الحق " Jus ad Bellum" وكذا إمكانيـــة اعتبارها نزاعا مسلحا وإمكانية أن تشملها قواعد القانون الدولي الإنساني في ظل القواعد القانونية المؤطـرة لـ" Jus in Bello".

Résumé:

The war field has witnessed a great leap with the technological and digital transformation that the world is experiencing today, as the means of war have developed thanks to this transformation in an important part from direct battles, to others managed through an electronic virtual world, the danger of which may exceed previous forms of war.

Accordingly, electronic and cyber warfare have become new types of weapons in the current era, capable of causing massive and large-scale damage to the vital infrastructure of a country, and represent another facet of force that countries may resort to in their battles, after the traditional means of using force have undergone change. Thanks to the developments. This requires the international community to reach some consensus on the meaning of cyber war, and an international agreement to govern it.

In this analytical paper, we will examine the question of whether cyber-attacks can be considered, amounting to the real level of war, and the legality of resorting to them within the framework of international law with regard to the right to use force within the framework of the legal rules framing this right "Jus ad Bellum" as well as the possibility of considering it a conflict armed and the possibility of being covered by the rules of international humanitarian law in light of the legal rules framing Jus in Bello.

المقدمة

أصبح الفضاء السيبراني اليوم مجالا جديدا لتتبع العمليات العسكرية، ماجعله يبرز كفضاء جديد للحرب، بعد أن أحدث التطور الإلكتروني والرقمي المتسارع، نقلة نوعية الأسلحة والوسائل المستعملة في الحروب، وشن الهجمات على دول أخرى، ونقل العمليات الحربية إلى الفضاء الافتراضي الإلكتروني.

وقد أبدى متخصصو الشؤون الأمنية الدولية، ومنذ منتصف التسعينيات، اهتمامهم بالحرب السيبرانية كحرب قائمة بذاتها، لكن الموضوع استبعد من الأجندة الأمنية عقب هجمات 11 سبتمبر على الولايات المتحدة. ليعود ويطرح من جديد عام 2007، عندما عانت إستونيا، الدولة العضو في حلف الناتو، من هجمات سيبرانية واسعة النطاق، من جهات فاعلة غير دولية من أصل روسي، واحتلت بعدها العمليات السيبرانية في العالم الموالي، مكانة بارزة في النزاع المسلح الدولي بين روسيا وجورجيا.[196]

[196] Michael N. Schmitt: The law of cyber warfare: Quo Vadis?. Stanford Law & Policy Review. Vol. 25:269. 2014. P: 269.

ونظرا لحداثة هذا النوع، من الأسلحة والاثار المأساوية التي أصابت وتمس الإنسانية جراء استخدامه، استوجب معه البحث في مشروعيتها، ومدى مطابقتها لقواعد القانون الدولي، لاسيما مع عدم وجود اتفاق دولي يحظر أو يقيد استخدامها، والبحث من جهة أخرى عن مكانة الحرب السيبرانية في القانون الدولي الإنساني تحديدا، ومدى إمكانية سريان قواعده عليها.

وعلى هذا الأساس، سنبحث في الحرب السيبرانية من زاويتين في القانون الدولي: القانون الذي يحكم اللجوء إلى القوة بين الدول (Jus ad Bellum)، والقانون الدولي الإنساني فيما يتعلق بالنزاعات المسلحة (Jus in Bello)، وبالتالي سيتم تقسيم هذا الموضوع إلى محورين: الأول حول مدى مشروعية الاسلحة السيبرانية في نطاق القواعد القانونية الدولية، وسيعالج الثاني إمكانية تطبيق القانون الدولي الانساني على الحرب السيبرانية.

المحور الأول: الأسلحة السيبرانية ومدى مشروعيتها في نطاق قواعد القانون الدولي

تتميز الحرب السيبرانية عن غيرها من الحروب التقليدية، باعتمادهاعلى فضاء افتراضي غير مادي وهو الفضاء السيبراني، لتنفيذ العمليات العدائية والهجمات. وهو فضاء يتشابك ويلتقي بعالمنا المادي، ويتفاعل معه بشكل في غاية التعقيد، مع تحقيق درجة تكامل كبيرة بينهما. كما يتميز الفضاء السيبراني، بغياب الحدود الجغرافية وغياب عنصر الزمن، وهو مايزيد من خطورته.[197]

وكتعريف للفضاء السيبراني فيقصد به: "البيانات والشبكات الالكترونية المتصلة، والأشخاص الذين يستخدمونها، حيث تعد هذه العناصر العامل المشترك في جميع محاور استخدام الفضاء السيبراني.[198] كما ويمكن وصف "الفضاء السيبراني" بأنه شبكة مترابطة عالميًا من المعلومات الرقمية والبنى التحتية للاتصالات، بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعلومات المقيمة فيها.[199]

---

[197] **ختال هاجر: الوضع القانوني للحرب السيبرانية على ضوء قواعد القانون الدولي. مجلة التواصل في الاقتصاد والإدارة والقانون. جامعة باجي مختار، عنابة، الجزائر. المجلد 25 -العدد 03 - سبتمبر 2019. ص: 159.**

[198] **ختال هاجر: نفس المرجع.**

[199] **Nils Melzer : Cyberwarfare and International Law. United Nations Institute for Disarmament Research(UNIDIR) RESOURCES. 2011. P :4.**

أما بالنسبة لتعريف الحرب السيبرانية فلا يوجد تعريف عالمي متفق عليه حول هذا النوع من الحرب. فوفقا لمؤسسة "RAND" الأمريكية، فالحرب السيبرانية: "تتضمن الإجراءات التي تتخذها دولة قومية أو منظمة دولية للهجوم ومحاولة إتلاف أجهزة الحاسوب أو شبكات المعلومات الخاصة بدولة أخرى".[200]

وتوصف العمليات السيبرانية بوجه عام بأنها عمليات تشن ضد أو عبر حاسوب أو نظام حاسوبي بواسطة تيار البيانات. وقد تهدف هذه البيانات إلى تحقيق أغراض مختلفة تضم على سبيل المثال اختراق نظام معين وجمع أو نقل أو تدمير أو تغيير أو تشفير البيانات، أو إجراء تعديل العمليات التي يتحكم فيها الجهاز الحاسوبي المخترق أو التلاعب بهذه العمليات. ويمكن على هذا النحو استخدام هذه الوسائل لتدمير أو تعديل أو تعطيل مجموعة متنوعة من الأهداف في العالم الحقيقي، كالبنى الأساسية، حيث تثير النتائج المحتملة لهذه العمليات مخاوف كبيرة على الصعيد الإنساني.[201]

فالحرب السيبرانية تعتمد على تكنولوجيا المعلومات والاتصالات، والاعتماد على الشبكات الذكية وغيرها من أنظمة المراقبة والرصد عن طريق الأنترنيت. ومفهومها يشمل استهداف القدرات والأنظمة العسكرية واستهداف البنية التحتية الحيوية للمجتمع، بما في ذلك الشبكات الذكية وشبكات المراقبة الاشرافية وحيازة البيانات التي تسمح لها بالعمل والدفاع عن أمنها.[202] وبالتالي، على سبيل المثال، فإن إصابة شبكة حاسوب الخصم المحارب بفيروس ضار من شأنه أن تشكل عملاً من أعمال الحرب السيبرانية، في حين أن القصف الجوي لقيادة عسكرية إلكترونية لن يكون كذلك.[203]

من جهته، يرى "Paul N Cornish" – وهو مدير سابق للمركز العالمي لقدرات الأمن السيبراني بجامعة أكسفورد- في تقريره حول الحرب السيبرانية أنه يمكن أن تكون الحرب السيبرانية صراعا بين الدول، كما ويمكنها أن تشمل أيضا جهات فاعلة غير حكومية بطرق مختلفة. وعلى مستوى أهداف هذه الحرب، فيمكن أن تكون عسكرية أو صناعية أو مدنية، كما وتصعب القدرة على التنبؤ في الحرب السيبرانية.[204]

---

[200] **Zain Dar: Cyber Warfare and International Law. Jacobs University Bremen;International Law. Spring 2019. P: 2.**

[201] **ختال هاجر: الوضع القانوني للحرب السيبرانية على ضوء قواعد القانون الدولي. ص: 160.**

[202] **بن تغري موسى: الحرب السيرانية والقانون الدولي الانساني. مجلة الاجتهاد القضائي. المجلد 12- عدد خاص (العدد التسلسلي 22) أبريل 2020. مختبر أثر الاجتهاد القضائي على حركة التشريع- جامعة محمد خيضر بسكرة- الجزائر. ص: 200.**

[203] **Nils Melzer : Cyberwarfare and International Law. Op,cit . P :4.**

[204] **Zain Dar: Cyber Warfare and International Law. Op,cit. P: 3/4.**

واستنادا إلى طريقة Action-Action، يمكن تعريف الحرب السيبرانية على أنها: "استخدام الهجمات الإلكترونية بقصد شبيه بالحرب". وسبب استخدام مصطلح الحرب، وليس أي مصطلحات أخرى يرجع إلى حقيقة أن هذه الهجمات لها نفس الركائز التي تتحقق بها الحرب مثل النية (المنفعة الشخصية أو النفسية)، لذلك فإن كلمة "الحرب" تظل ثابتة.[205]

والبحث في مجمل التعريفات الخاصة بالحرب السيبرانية، يتبين أنه لا يوجد تعريف واحد يدعم مفهوم هذه الحرب بشكل كامل. فبعض التعريفات واسعة للغاية، والبعض الآخر يفتقر إلى الجهات الفاعلة المعنية، للوصول إلى نموذج محدد للحرب السيبرانية يمكن تطبيق القوانين الدولية عليه.

بالنسبة لأشكال الحرب السيبرانية، فلا يتوفر اليوم بصورة رسمية نظام لتصنيف أنواع العمليات ضمن وعبر الفضاء الالكتروني. فقد دفع التطور في مجال الفضاء الالكتروني إلى بروز ترسانة غير تقليدية لأسلحة الكترونية متعددة؛ كالفيروسات، والاختراق، وسرقة المعلومات، والتشويش، الحرب عن طريق التحكم عن بعد بأسلحة سواء جوية أو برية أو بحرية... وتعد الطائرات بلا طيار(drones) مثالا بارزا على منظومات الأسلحة التي يتم التحكم بها عن بعد، وهي نظام المركبة الهوائية الموجهة التي يتم السيطرة عليها، وعلى ما تحمله من معدات، وعلى سطوح التحكم في أدائها من بعد.[206]

ويمكن للهجمات السيبرانية أن تعطل المنشآت الحكومية والبنية التحتية المدنية مثل شبكات الكهرباء والسكك الحديدية وخطوط أنابيب النفط وشركات الطيران وأنظمة النقل والأسواق المالية وما إلى ذلك، وبالتالي تهدد حياة الدولة.[207] في الوقت الحاضر، نظرًا لأهمية هذه القضية، زعمت أجهزة الاستخبارات في الولايات المتحدة رسميًا أن مايقرب من 20 إلى 30 دولة تقوم بتشكيل وحدات خاصة للحرب السيبرانية، وأيضًا يضع حلف الناتو الحرب السيبرانية كأولويات جديدة على جدول أعماله.[208]

---

[205] Zain Dar: Ibid. P: 5.

[206] ختال هاجر: الوضع القانوني للحرب السيبرانية على ضوء قواعد القانون الدولي. مرجع سابق. ص: 161/160.

[207] Nazanin Baradaran & Homayoun Habibi: Cyber Warfare and Self - Defense from the Perspective of International Law. Journal of Politics and Law; Published by Canadian Center of Science and Education. Vol. 10, No. 4; 2017. P: 40.

[208] Ibid. P: 41.

بالانتقال إلى بحث مشروعية الحرب السيبرانية من وجهة القانون الدولي في إطار "Jus ad Bellum "، فإن هذه القواعد القانونية، تنظم الحق في استخدام القوة في العلاقات بين الدول، ويعد ميثاق الأمم المتحدة مصدر مهم لـ "Jus ad Bellum" في العصر الحديث.

ومنذ ظهور العمليات السيبرانية، سعت الدول وجانب من الفقه الدولي، إلى تحديد العتبة التي يصبح عندها الفعل "استخداما للقوة"، على اعتبار أن العمليات السيبرانية، قد تسبب هي الأخرى شأنها شأن عمليات الحرب التقليدية، الضرر أو الإصابات المادية والجسدية. [209]

ونظرا لأهمية موضوع هذه القضية في النقاش الميداني حول الحق في استعمال (القوة) في الحرب، فإن مبدأ عدم اللجوء إلى القوة كأحد أهم مبادئ ميثاق الأمم المتحدة تعتبره المادة 2 الفقرة 4 من الميثاق، قوة عسكرية فقط، ولا يشمل الحظر الوارد فيها استخدامها فحسب، بل يشمل أيضا التهديد باستخدامها. والسؤال الذي يطرح نفسه في إطار هذا القانون هو ما إذا كان يمكن أيضا اعتباره استخدام الفضاء السيبراني لشن هجمات إلكترونية، استخداما للقوة. فالميثاق الأممي ينص على أنه لا ينبغي التسامح مع الأعمال التي تستخدم "القوة"، مع الإشارة إلى استعماله لمصطلح القوة بشكل فضفاض، وهذه إحدى الاشكاليات التي يثيرها هذا الميثاق.

إلى جانب ذلك، تبرز قضية أخرى وهي أنه طالما ليست هناك إصابات جسدية، فإن مثل هذه العمليات يصعب الإشارة إليها على أنها "قوة". لكن مع ذلك فإن العمليات السيبرانية يمكن أن تؤدي أيضا إلى نزاعات مسلحة. ويمكن في هذا الباب فقط طرح مسألة عدم شرعية مثل هذه العمليات. الشيء نفسه ينطبق على كلمة "هجوم مسلح"، نظرًا لعدم وجود حدود محددة تُعتبر عندها العملية السيبرانية قوة أو هجومًا مسلحًا، فلا يمكن لأحد التأكد من ذلك. [210]

بالمقابل، فإنه في ظل عدم وجود تعريف دقيق لما هو استخدام القوة، إلا أن بعض العوامل راسخة، على سبيل المثال، تأتي الهجمات بالأسلحة التقليدية في سياق الفقرة 4 من هذه المادة. علاوة على ذلك، فإن الهجمات السيبرانية، التي تُستخدم لغرض الإضرار المباشر بالممتلكات المادية أو التسبب في أضرار بشرية أو وفاة، يتم تصنيفها بشكل معقول على أنها استخدام للقوة. وبالتالي إذا كانت النتائج مشابهة لتأثيرات هجوم

---

[209] Michael N. Schmitt: The law of cyber warfare: Quo Vadis? Op,cit. P:279.

[210] Zain Dar: Cyber Warfare and International Law. Op,cit. P: 6.

مسلح، فإن تطوير مفهوم القوة لهذه التدابير يكون معقولا، وإلا حدث فعل غير مشروع وفقا للقانون الدولي، والذي ينبغي اللجوء إليه إلى أحكام القانون الدولي الأخرى بخلاف حظر استخدام القوة. لكن مع هذا، لازالت إمكانية تنفيذ الفقرة 4 من المادة 2 من الميثاق في الحرب السيبرانية تخلق مشاكل جدية في تفسير الفرق بين القوة والإكراه.[211]

هذا المبدأ المتعلق باستخدام القوة، مصحوب ببعض الاستثناءات التي أنشأها القانون الدولي العرفي، إلى جانب قرارات مجلس الأمن في إطار الفصل السابع، وحالة الدفاع عن النفس على النحو المنصوص عليه في المادة (51) من الميثاق، حيث أنه بالنسبة للدولة الضحية توفر لها هذه المادة الحق في الدفاع المشروع عن النفس، شرط أن يصل استخدام القوة إلى عتبة "هجوم مسلح". لذا يطرح السؤال حول ما إذا كانت آثار الهجوم السيبراني وحدها تجعل حق الدفاع عن النفس في غياب الضرر البشري والمادي كافياً؟ إن القضايا الواردة في هذه المادة من الميثاق، والقانون الدولي العرفي تنص على الدفاع عن النفس. لكنهما يتفقان على أن ما يُنشئ حق الدفاع عن النفس هو الهجوم المسلح عليهما. ومن ثم، فإن تحديد الهجمات السيبرانية على أنها هجوم مسلح هو مسألة قانونية يجب دراستها والتحقيق فيها.[212]

لهذا، يتوجب على المجتمع الدولي التوصل إلى توافق في الآراء حول معنى هذه الأنشطة بموجب الميثاق، ولا سيما المادة (2 ف 4) التي تنظم استخدام القوة، والمادة (51) التي تنص على الحق في الدفاع عن النفس. وبالتالي، إذا كان عمل الدولة يعتبر استخداماً للقوة، وفقًا للمفهوم المنصوص عليه في فقرة المادة الأولى، فهو غير قانوني ما لم يكن ذلك من أجل تنفيذ حق بلد في إطار حق الدفاع الشرعي.[213]

سؤال معقد ومشكلة أخرى هو أن الهجمات على البنية التحتية الحيوية للدولة، والتي تسبب دمارًا أساسيًا ولكنها لم تسبب ضررًا بشريًا أو ماديًا ، هل يمكن اعتبارها هجومًا مسلحًا ومنح حق الدفاع عن النفس؟ تتطلب الإجابة على هذا السؤال أن نقول ما هي البنية التحتية الحيوية؟. فعلى الرغم من عدم وجود تعريف مقبول عالميا، إلا أن معظم التعاريف متفق عليها في هذه الحالات التي تعتبر فيها بعض الخدمات المعينة مثل الأمن،

---

[211] Nazanin Baradaran & Homayoun Habibi: Cyber Warfare and Self - Defense from the Perspective of International Law. Op,cit. P: 41/42.

[212] Nazanin Baradaran & Homayoun Habibi: Cyber Warfare and Self - Defense from the Perspective of International Law. Op,cit. P: 41/42.

[213] Ibid. P: 41.

الغذاء، المياه، النقل، المصارف والتمويل، الصحة، الطاقة، والخدمات العامة والحكومية، بمثابة بنى تحتية بالغة الأهمية. ومن هذا المنطلق ، يمكن القول إن الهجوم السيبراني على البنية التحتية الحيوية والذي يشل الإدارات الحكومية أو يتسبب في تدمير واسع النطاق فيها، يجب اعتباره هجومًا مسلحا، حتى لو لم يتسبب في أضرار مادية أو وفيات. فعلى سبيل المثال، يجب اعتبار أي هجوم على النظام المالي الحكومي من خلال تغيير أو إتلاف المعلومات التي تسبب خطرًا على الحياة الاقتصادية للدولة، هجومًا مسلحًا، وهذا ليس بسبب التدمير المادي، وإنما لكون هذه الهجمات تتسبب في تعطيل البنية التحتية للدولة وجعلها غير قادرة على الوصول إلى الأهداف التي تم إنشاؤها بسببها. لذلك يجب اعتبار مثل هذه الهجمات بمثابة هجوم مسلح.[214]

من زاوية أخرى، يمكن طرح سؤال عما إذا كان الهجوم الإلكتروني على البنية التحتية العسكرية لبلد ما هو هجوم مسلح؟

بالنظر إلى أثار هذا الهجوم ومدى تسببه في أضرار جسيمة، فسيكون لديه المعايير اللازمة للدفاع عن النفس، وليس من الضروري أن تكون هذه الأضرار خسائر مادية أو بشرية، ولكن تعطيل الخدمات الحكومية على نطاق واسع من شأنه أن يتسبب في إضعاف الحكومة وضعفها، سيكون كافيا أيضا. علاوة على ذلك، في كثير من الحالات ، يمكن أن يكون مثل هذا الهجوم بمثابة مقدمة لمتفجرات والهجوم الحركي، في مثل هذه الحالة سيخلق حق الدفاع الوقائي عن النفس.[215]

للإشارة، فإن الهجمات السيبرانية، غالبًا ما تكون متعددة الطبقات، وفيها التأثير المدمر الذي يحدث في الأنظمة، وتنفيذ التحميل، وإنتاج الآثار الضارة، وهذا قد يحدث في فترات زمنية مختلفة. فإذا تم تحديد الهجوم من خلال آثاره الضارة التي تشمل أيضًا التأثيرات الضعيفة للهجوم، يكون الهجوم متاحًا بمجرد تحقيق آثاره الضارة، بغض النظر عن وقت اختراق النظام أو تنفيذ الحمل. ومع ذلك، إذا أدركت الدولة أن أنظمتها تالفة، فيمكنها اعتماد تدابير إلكترونية دفاعية نشطة أو سلبية لتحييد التهديدات. قد تعتبر الدولة أيضا هذا

---

[214] Ibid. P: 42/43.

[215] Nazanin Baradaran & Homayoun Habibi: Cyber Warfare and Self - Defense from the Perspective of International Law. Op,cit. P: 43.

التأثير في الأنظمة بمثابة مقدمة لهجوم إلكتروني أو انفجار، إذا كانت المعلومات المتاحة تشير إلى أن هذا الهجوم جزء من هجوم عام.[216]

ومن أجل اللجوء إلى استخدام القوة، أو الدفاع عن النفس، يتوجب احترام معياري الضرورة والتناسب في القانون الدولي، إذ أن استخدام القوة من قبل الدولة من أجل تتنفيذ حقها في الدفاع عن النفس، الذي يخضع أيضًا لعمليات سيبرانية، يجب أن يكون ضروريا ومتناسبا، أي أن تدابير الدفاع عن النفس يجب أن تفي بهذين المعيارين.[217]

النقطة الأساسية في تحليل الضرورة في مجال الهجمات السيبرانية، هو وجود أو عدم وجود تدابير بديلة لا تصل إلى عتبة "استخدام القوة". فإذا كانت الإجراءات الدفاعية السيبرانية السلبية (التي تختلف عن التدابير الدفاعية النشطة) لإحباط الهجوم السيبراني بشكل موثوق وكامل عن طريق الإنترنت كافية، فإن الإجراءات الأخرى، سواء الإلكترونية أو الحركية، والمتفجرة، تعتبر استخداما غير قانوني للقوة. وبالمثل، إذا كانت العمليات السيبرانية النشطة التي لم تصل إلى استخدام القوة، كافية لصدهجوم إلكتروني، يتم حظر التدابير القسرية الإلكترونية، أو إجراءات التفجير البديلة، حيث يتم حظر المعايير الضرورية وعدم القيام بها. ومع ذلك، عندما تكون التدابير التي تعتبر استخداما مقيدا للقوة غير قادرة على هزيمة هجوم سيبراني، أو منع هجمات مستقبلية بمفردها، يتم تضمين العمليات الإلكترونية والحركية باعتبارها استخدامًا للقوة على أساس الحق المسموح به في الدفاع عن النفس.[218]

يقيم مبدأ التناسب مسألة مقدار القوة التي تتضمن أيضا القوة الإلكترونية المسموح بها، عندما تكون هناك ضرورة للدفاع. تحد هذه المعايير من النطاق، والمجال، والفاصل الزمني، وشدة رد الفعل الدفاعي. لكن هذه المعايير لاتحد من رد الفعل كمقدار القوة المستخدمة في الهجوم، نظرا لكون مقدار ومستوى القوة اللازمة لصد الهجوم بنجاح، يعتمد على الموقف.[219]

---

[216] **Ibid. P: 43.**

[217] **Ibid. P: 44.**

[218] **Nazanin Baradaran & Homayoun Habibi: Cyber Warfare and Self - Defense from the Perspective of International Law. Op,cit. P: 44.**

[219] **Ibid. P: 44.**

بالإضافة إلى القواعد القانونية المشار إليها سابقا، أشارت محكمة العدل الدولية في ست قضايا إلى قواعد مهمة من القانون الدولي العرفي والمبادئ العامة ذات الصلة باللجوء القانوني إلى استخدام القوة. فلا يجب أن يكون هناك هجوم مسلح أو هجوم مسلح مكافئ، فقط لتبرير استخدام القوة العسكرية للدفاع عن النفس، ولكن يجب أن يكون الهجوم كبيرًا؛ وأن يُنسب إلى الدولة التي يتم فيها الدفاع عن النفس؛ وأن يكون استخدام القوة هو الملاذ الأخير، وأن ينجح على الأرجح في تحقيق الدفاع؛ ويكون متناسبًا مع الضرر الذي لحق به.[220]

هذا، وتشير ممارسات الدول إلى أن قضية الإسناد يجب أن تقدم بأدلة واضحة ومقنعة. في حالة الهجمات الإلكترونية بشكل عام، يصعب العثور على أدلة مقنعة، نظرًا لعدم الكشف عن هوية التكنولوجيا المعنية، وقد يكون من الصعب للغاية إسناد هجوم إلكتروني إلى دولة معينة. في حين أن الدولة الضحية قد تنجح في نهاية المطاف في تتبع هجوم إلكتروني إلى خادم معين في دولة أخرى، لكن قد تستغرق عملية وقتًا طويلاً، وحتى في هذه الحالة قد يكون من المستحيل تحديد الكيان أو الفرد الذي يوجه الهجوم بشكل نهائي. وبالتالي هناك مشكلة في إثبات أن الهجوم المضاد يمكن أن يحقق هدفًا دفاعيًا.[221]

من جهة أخرى، فإن الهجوم السيبراني أو التجسس الإلكتروني حتى وإن كان لا يرقى إلى مستوى الهجوم المسلح، فهذا لا يعني أن القانون الدولي يبيح هذه الأفعال. فهو يحظر التدخل في المجال الاقتصادي للدولة، أو المجال الجوي أو الفضاء البحري أو الفضاء الإقليمي، حتى لو لم يكن محظورًا بموجب المادة (2 ف4) من ميثاق الأمم المتحدة، وذلك بموجب المبدأ العام لعدم التدخل. تتجلى هذه الحقيقة في عدد من المعاهدات وقرارات الأمم المتحدة، وقرارات محكمة العدل الدولية، التي تدين الإكراه أو التدخل الذي لا يرقى إلى مستوى استخدام القوة. فقد أشارت محكمة العدل الدولية إلى بعض هذا السلوكات على أنها "أشكال أقل خطورة" للقوة، تنتهك مبدأ عدم التدخل مع عدم المساس بحقوق الضحية بموجب المادة (51). ودعماً لذلك ، أشارت المحكمة إلى إعلان الجمعية العامة للأمم المتحدة بشأن العلاقات الودية، واتفاقية منظمة الدول

[220] Mary Ellen O'Connell: Cyber Security and International Law. International Law: Meeting Summary. Chatham House. London. 29 May 2012. P: 6.

[221] Mary Ellen O'Connell: Ibid. P: 7.

الأمريكية بشأن حقوق وواجبات الدول في حالة نشوب حرب أهلية، ومصادر موثوقة أخرى لمحتوى مبدأ عدم التدخل.[222]

ما الذي يمكن فعله للرد على انتهاكات مبدأ عدم التدخل؟ ما هي التدابير المتاحة للرد عليها بشكل قانوني إذا كان القانون الدولي يثير حواجز كبيرة أمام استخدام الأسلحة السيبرانية والدفاع عن الفضاء السيبراني من الهجمات الإلكترونية من خلال استخدام القوة؟.

بشكل عام، يدعم القانون الدولي تنظيم الفضاء السيبراني كمجال اقتصادي واتصالات، ويحتوي على وسائل قسرية للرد بشكل قانوني على الاستفزازات السيبرانية بجميع أنواعها. ونفس هذه التدابير القسرية التي يسمح باستخدامها ضد الانتهاكات الاقتصادية وانتهاكات معاهدات الحد من الأسلحة، سيكون قانونيا بشكل عام، للاستخدام في حالة وقوع هجوم سيبراني.[223]

زيادة على ذلك، فإنه وبموجب قانون الحياد، لازالت تطرح الأسئلة حول ما إذا كان بإمكان المتحاربين استخدام البنية التحتية للاتصالات السلكية واللاسلكية للدول المحايدة بشكل قانوني بغرض شن هجمات سيبرانية، وما هي مسؤوليات الدول "المحايدة" فيما يتعلق بالأطراف غير الحكومية التي تشن هجمات من الداخل أو عبر أراضيها أو بنيتها التحتية.[224]

للإشارة، فقد روجت روسيا لمعاهدة على غرار اتفاقية الأسلحة الكيميائية لتنظيم الفضاء السيبراني لعدد من السنوات. في خطاب ألقاه في 18 مارس 2012 ، أوضح "فلاديسلاف ب. شيرستيوك"، نائب سكرتير مجلس الأمن الروسي، ما وصفه بمواقف روسيا الأساسية بشأن نزع السلاح في الفضاء الإلكتروني. ستحظر المعاهدة المقترحة لروسيا أي بلد من تضمين رموز أو دوائر خبيثة سراً يمكن تفعيلها لاحقًا من بعيد في حالة نشوب حرب.[225] لكن لم يكتب لهذه المبادرة النجاح.

---

[222] Mary Ellen O'Connell: Cyber Security and International Law. Op,cit. P: 7.

[223] Ibid. P: 7/8.

[224] Nils Melzer : Cyberwarfare and International Law. Op,cit. P :3.

[225] Mary Ellen O'Connell: Ibid. P: 9.

مما سبق يمكن القول أنه بموجب القانون المنظم للجوء إلى القوة بين الدول (jus ad bellum)، سيتعين تحديد الظروف، إن وجدت، التي يمكن أن ترقى فيها العمليات السيبرانية إلى: [226]

(أ) تهديد غير مشروع دوليًا أو استخدام "القوة"؛

(ب) "هجوم مسلح" يبرر اللجوء إلى القوة الضرورية والمتناسبة دفاعاً عن النفس؛

(ج) "تهديد للسلم والأمن الدوليين" أو "خرق للسلام" رهنا بتدخل مجلس الأمن التابع للأمم المتحدة.

المحور الثاني: إمكانية تطبيق القانون الدولي الانساني على الحرب السيبرانية

بموجب قانون النزاع المسلح (jus in bello)، المشار إليه هنا بالقانون الدولي الإنساني (IHL)، يجب التمييز بين "الحرب السيبرانية" والظواهر التي لا يحكمها القانون الدولي الإنساني بالضرورة، مثل "الجريمة الإلكترونية"[227] ومن المصادر المهمة لـه اتفاقيات جنيف الأربع، وبروتكوليها، واللوائح التي أدخلت في اتفاقية لاهاي الرابعة وسلسلة من المعاهدات الأخرى.

وارتباطا بهذا القانون، تثير مسألة ما إذا كانت العمليات الإلكترونية يمكن أن ترقى إلى مستوى لحرب أو النزاع المسلح أو العدوان، أسئلة أولية عن التعريف والمصطلحات.

في الوقت الحالي، وكما تمت الاشارة سلفا، هناك صعوبة في تحديد مفاهيم "الحرب السيبرانية" و"الأعمال العدائية السيبرانية" و"النزاع السيبراني" بشكل رسمي لأغراض القانون الدولي. التعريف القانوني الوحيد الموجود، ماجاءت به معاهدة صادرة عن منظمة شنغهاي للتعاون الإقليمية، يتعلق بالمفهوم الأوسع لـ "حرب المعلومات"، والتي يتم تعريفها على أنها: المواجهة بين دولتين أو أكثر في فضاء المعلومات تهدف إلى إتلاف أنظمة المعلومات والعمليات والموارد والهياكل الحرجة وغيرها، وتقويض النظم السياسية والاقتصادية والاجتماعية، وغسيل الدماغ النفسي الجماعي لزعزعة استقرار المجتمع والدولة، وكذلك لإجبار الدولة على اتخاذ قرارات لصالح طرف معارض.[228]

ونظرا لكون مصطلح "حرب المعلومات" غالبًا ما يستخدم بشكل غير دقيق كمرادف لـ "عمليات المعلومات"، في حين أن هذه الأخيرة يمكن أن تحدث في زمني السلم والحرب، أما الأولى فتشير حصريا إلى العمليات الإعلامية التي يتم إجراؤها في حالات النزاع المسلح، ويستبعد العمليات الإعلامية التي تحدث في

---

[226] Nils Melzer : Cyberwarfare and International Law. Op,cit. P :3.

[227] Ibid.

[228] Ibid. P :22.

أوقات السلم. وبالتالي عند تطبيقه على السياق الأكثر تحديدا للعمليات السيبرانية، فإن هذا يعني أن استخدام مصطلح "الحرب السيبرانية" و"الأعمال العدائية السيبرانية" و"النزاع السيبراني" يجب أن يقتصر على النزاعات المسلحة بالمعنى المقصود في القانون الدولي الإنساني.[229]

مما له أهمية خاصة حقيقة، أن القانون الدولي الإنساني في شقه الذي يحكم سير الأعمال العدائية، يقوم على نموذج تكون فيه معظم العواقب الوخيمة التي يسعى إلى التخفيف من أضرارها، مدمرة أو ضارة جسديا، ووفقا لذلك تنحرف العمليات السيبرانية عن هذا النموذج الأساسي. فقد يتم إطلاقها بعيدا عن ساحة المعركة النشطة، مما يثير مخاوف بشأن الحدود العملية والمعيارية للنزاع المسلح. لاسيما وأن هذه العمليات تصاحبها القدرة على إخفاء أو انتحال أصل العملية الإلكترونية، مايتسبب في تعقيد خيارات الاستجابة المتاحة لأولئك المستهدفين. ويمكن أن تؤدي آثارها إلى عواقب وخيمة على الدولة، وإن كانت غير مدمرة أو ضارة على السكان المدنيين. وبالتالي يصعب مع هذا الوضع التوصيف القانوني للنزاع، والقانون الواجب التطبيق.[230]

فعندما يؤدي استخدام الأجهزة الرقمية الهجومية إلى الإصابة أو الوفاة أو التلف أو التدمير، يصبح القانون الذي يحكم النزاع المسلح ذا صلة. لكن عندما يتم نشر أو زرع سلاح إلكتروني مثلا، فهل هذا شيء مختلف تماما عن السلاح الحركي؟ دافع فقهاء القانون الدولي عن مفاهيم مثل "النزاع المسلح" و"الهجوم المسلح" على مر السنين. ومع ذلك، هناك إجماع عام على أننا بحاجة إلى النظر في العواقب، أو في السياق السيبراني، العواقب غير المباشرة لنشر البرامج الضارة التي ينظمها القانون الدولي.[231]

على سبيل المثال، إذا قامت الدولة "أ" بنشر البرامج الضارة في البلد "ب" بهدف تدمير البنية التحتية الحيوية مثل التحكم في الطيران المدني والشبكات الوطنية - فسوف تتحطم الطائرات وتؤدي إلى الوفاة والإصابة والأضرار. إذا كان هذا ناتجًا عن برامج ضارة رقمية وتسبب في ضرر إلى حد يعادل هجومًا مسلحًا بإلقاء قنبلة على نفس الأهداف ، فلا يبدو أن هناك أي سبب للتمييز بين البرامج الضارة والأسلحة التقليدية. إلى هذا الحد، هناك إمكانية لتطبيق قانون النزاعات المسلحة. وعلى أساس ذلك، فإذا فهمنا كيف ينطبق هذا القانون على الحرب السيبرانية المحتملة، فيمكننا تطبيقه.[232]

---

[229] Nils Melzer : Cyberwarfare and International Law. Op,cit. P :22.

[230] Michael N. Schmitt: The law of cyber warfare: QUO VADIS?. Op,cit. P:289.

[231] Mary Ellen O'Connell: Cyber Security and International Law. Op,cit. P: 10.

[232] Mary Ellen O'Connell: Cyber Security and International Law. Op,cit. P: 11.

في الواقع، يمكن وصف التهديدات الأمنية المنبثقة من الفضاء السيبراني، والتي لا تصل إلى عتبة النزاع المسلح على أنها "جريمة إلكترونية" أو "عمليات إلكترونية"، أو عند الاقتضاء "إرهاب إلكتروني" أو "قرصنة إلكترونية"، ولكن لا ينبغي الإشارة إليها بمصطلحات تثير الشك وعدم اليقين بشأن انطباق قانون النزاعات المسلحة. وبالتالي فاليوم، يبدو أنه لا جدال في أن القانون الدولي الإنساني ينطبق على العمليات السيبرانية التي يتم تنفيذها في سياق نزاع مسلح دولي أو غير دولي موجود مسبقًا.[233] لهذا يتوقع القانون الدولي الإنساني بوضوح، تطبيق قواعده ومبادئه على أساليب ووسائل الحرب المطورة حديثا، وإن كان تعامله مع طبيعة هذه الأساليب والوسائل غير دقيق، لكنه يركز على السياق الذي تستخدم فيه، وهو الذي تخضع بموجبه لقواعد هذا القانون ومبادئه. فاعتبار العملية السيبرانية على أنها نُفّذت في سياق نزاع مسلح، لا يعتمد بالضرورة على الارتباط الإقليمي لهذه العملية، وإنما على ما إذا كانت تُنفَّذ لأسباب تتعلق بنزاع مسلح، أو حسب المحكمة الجنائية الدولية ليوغوسلافيا السابقة (ICTY)، كان لها "صلة" بنزاع مسلح مستمر. وهذا يعني أيضا أن العمليات السيبرانية التي يتم إجراؤها لأسباب لا علاقة لها بنزاع مسلح (عدم وجود رابط)، قد تعتبر جريمة إلكترونية وما إلى ذلك، ولا تخضع وفقا لذلك للقانون الدولي الإنساني، حتى لو تم تنفيذها من قبل طرف محارب، أو داخل إقليم المتضررة من نزاع مسلح.[234]

وبالتالي يشترط لتطبيق القانون الدولي الانساني على هذه النزاع والعمليات السيبرانبة أن تنفذ العمليات في سياق نزاع مسلح وكانت مرتبطة به. أي إذا قام أحد أطراف النزاع بالتزامن مع القصف المدفعي وغيره، قامت أيضا بإطلاق هجوم إلكتروني على النظم الحاسوبية لخصمه، فهنا الهجوم السيبراني يوصف بهجوم في إطار نزاع مسلح وبالتالي تنطبق عليه قواعد القانون الدولي الانساني، كمبدأ التمييز وتحريم ضرب المدنيين والأعيان المدنية ومنع الأضرار غير المبررة وغيرها.[235]

وبناء على ذلك، فإن وسائل وأساليب الحرب التي تتكون من عمليات سيبرانية، قد ترقى إلى مستوى نزاع مسلح أو تُجرى في سياق نزاع مسلح ، بالمعنى المقصود في القانون الدولي الإنساني، خاصة في ظل التكلفة الإنسانية المحتملة لهذه الهجمات. فعندما تتعرض أجهزة الكمبيوتر أو الشبكات التابعة لدولة ما للهجوم أو التسلل أو حجبها، فقد يكون هناك خطر حرمان المدنيين من الضروريات الأساسية مثل مياه الشرب والرعاية

---

[233] **Nils Melzer : Cyberwarfare and International Law. Op,cit. P :22.**

[234] **Ibid. P :23.**

[235] **بن تغري موسى: الحرب السيرانية والقانون الدولي الانساني. مرجع سابق. ص: 203.**

الطبية والكهرباء... كما أنه إذا كانت أنظمة GPS مشلولة ، فقد يكون هناك خطر وقوع إصابات بين المدنيين - على سبيل المثال، من خلال تعطيل عمليات طيران مروحيات الإنقاذ التي تنقذ الأرواح. السدود والمحطات النووية وأنظمة التحكم في الطائرات، بسبب اعتمادها على أجهزة الكمبيوتر، هي أيضًا عرضة للهجمات السيبرانية.[236]

من جهة أخرى فإن الاهداف العسكرية والتي قد تكون لها تأثيرات تلحق بالبنية الأساسية المدنية، يجب أن تأخذ في الاعتبار مبدأ التناسب، حتى لاتترك مثل هذه الحروب بلا قواعد ولا نظم.[237]

على مستوى إمكانية إدراج الحرب السيبرانية ضمن مفهوم العدوان، فبالقياس إلى استخدام أسلحة الفضاء السيبراني، نجد أنها تمثل نوعا من استخدام القوة ذات الطابع المرن أو الإلكتروني التي ينتج عنها نفس نتائج استخدام القوة بمفهومها التقليدي. مايسمح بإدراج الحرب الفيروسية المعلوماتية التي تتم في الفضاء السيبراني ضمن مفهوم العدوان، لاعتبارات عديدة أهمها أن التطور الحاصل اليوم في التكنولوجيا العسكرية، أدى إلى تجاوز المفهوم التقليدي والجامد لجريمة العدوان كما حددها نظام روما المنشئ للمحكمة الجنائية الدولية في مادته 8 مكرر.[238]وعلى هذا الأساس ارتقى به بعض المختصين في القانون الدولي ومنهم الدكتور محمد سعادي إلى العدوان مسلح، قياساعلى استعمال الفيروسات المعلوماتية بالفيروسات الجرثومية المستعملة كسلاح بيولوجي ضد الدول. وبذلك عد الفيروس الالكتروني كالفيروس البيولوجي سلاحا جديدا يستخدم في معركة مفتوحة وميدان معركة غير معروفة المعالم، وتكون أثاره عشوائية.[239]

لكن تبقى هناك مشكلة تتعلق بمسألة إسناد هذا الهجوم السيبراني، حتى يحق للدولة التصرف دفاعا عن النفس فيما يتعلق بهجوم مسلح (حركي أو غير ذلك)،[240]مثل الهجوم الالكتروني على انتخابات 2016 الأمريكية والذي كان يعتبر عملاً من أعمال روسيا وكيف كان من الصعب إلقاء اللوم على أي طرف أو اتخاذه اي فعل.[241] وترتيب المسؤولية الدولية والجنائية عن الهجوم. فمشكلة الإسناد هذه، تسبب صعوبات من قبيل: من يهاجم وعلى أي أساس؟

---

236 ICRC : Cyberwarfare and international humanitarian law: the ICRC's position. 06/2013. P : 1.

237 بن تغري موسى: الحرب السيرانية والقانون الدولي الانساني. مرجع سابق. ص: 207.

238 ختال هاجر: الوضع القانوني للحرب السيبرانية على ضوء قواعد القانون الدولي. مرجع سابق. ص: 164.

239 نفس المرجع. ص: 165.

240 Mary Ellen O'Connell: Cyber Security and International Law. Op,cit. P: 11.

241 Zain Dar: Cyber Warfare and International Law. Op,cit. P: 8.

إذا كان الهجوم من قبل جهات غير حكومية، فهل يحصلون على أي دعم من الدولة؟؛ وإذا كان الأمر كذلك، فما درجة المشاركة؟. هذه الأسئلة مهمة حتى نتمكن من تطوير قواعد قانونية قوية، والاستعداد إذا حدث ذلك في مرحلة ما في المستقبل.[242]

وفي محاولة منه لتحديد معالم الحرب السيبرانية، أصدر حلف الناتو، دليل تالين "Tallinn Manuel"[243] الخاص بتطبيق القانون الدولي على الحرب السيبرانية، الذي رصد مختلف جوانب هذه الحرب والمبادئ الحاكمة لها في ظل المتغيرات الجديدة.[244] كما ويوضح كيفية تطبيق قواعد القانون الدولي الإنساني في هذا المجال.[245] لهذا فهو يعد خطوة مهمة نحو التأكيد على أهمية القانون الدولي الإنساني في مثل هذا النوع من النزاعات، طالما تندرج ضمن النزاعات المسلحة.[246]

ونأمل أن يساهم هذا الدليل بشكل مفيد في مزيد من المناقشة بين الدول حول هذه القضايا الصعبة، وأن تضمن الدول والجماعات المسلحة من غير الدول أن تكون العمليات السيبرانية، في النزاع المسلح متوافقة مع التزاماتها الدولية.[247]

وبالتالي، فخضوع أو عدم خضوع الهجمات السيبرانية للقانون الدولي الإنساني إنما يعتمد على طبيعتها وعلى النتائج المتوقعة منها، فالوسائل التي تستخدم لإحداث الأذى أو القتل أو الدمار هي أعمال غير إنسانية بغض النظر عن الوسيلة أو الطريقة التي استخدمت، وهو مايجعلها خاضعة لأحكام القانون الدولي الإنساني.

الخاتمة

يتبين مما سبق، أنه ونظرا لتطور أساليب الحرب السيبرانية بشكل متزايد مع تقدم القدرات التكنولوجية في مختلف البلدان، فهذا يستدعي ضرورة مواكبة القانون الدولي لهذه المستجدات، من خلال تنظيم قوانين محددة في هذا المجال جنبا إلى جنب مع التطورات الحاصلة، لاسيما وأنه في الوقت الراهن وفي غياب نص

---

[242] Mary Ellen O'Connell: Cyber Security and International Law. Op,cit. P: 11.

[243] أطلق مركز التميز للدفاع الإلكتروني التعاوني التابع لحلف الناتو مشروعًا بحثيًا كبيراً في أواخر عام 2009 لفحص القانون الدولي العام الذي يحكم الحرب الإلكترونية. أمضى عشرون من الأكاديميين والممارسين القانونيين من الطراز العالمي ("مجموعة الخبراء الدولية") السنوات الثلاث التالية في صياغة دليل تالين للقانون الدولي المطبق على الحرب الإلكترونية.

(Michael N. Schmitt: The law of cyber warfare: QUO VADIS?. Op,cit. P:270).

[244] بن تغري موسى: الحرب السيرانية والقانون الدولي الانساني. مرجع سابق. ص: 210.

[245] ICRC : Cyberwarfare and international humanitarian law.Op,cit. P : 2.

[246] Ibid. P : 1.

[247] Ibid. P : 2.

قانوني يؤطر هذا المجال، تنشأ العديد من الأسئلة والقضايا التي قد يكون من الصعب التعامل معها مثل كيف يمكن للمصطلحات الحالية العمل مع النظام السيبراني، ومدى قابليتها للتطبيق، وكيف تؤثر على مختلف الجهات الفاعلة، وغيرها من الأسئلة المختلفة.

لهذا تقترح هذه الورقة مجموعة من التوصيات تتمثل في:

1- ضرورة إدراج حرب الفيروسات المعلوماتية التي تتم في الفضاء السيبراني ضمن مفهوم العدوان ، وان للدول المتضررة من هذا العدوان حق الدفاع الشرعي المنصوص عليه في المادة 51 من ميثاق الامم المتحدة

2- تطوير اتفاقيات القانون الدولي الانساني القائمة وجعلها أكثر قابلية لتشمل ، في التنظيم، كل انواع الهجمات السيبرانية وكل انواع المخاطر والاضرار الناتجة عن هذه الهجمات.

3- تنظيم الدول العربية صفوفها، بمساهمة من الجهات الفاعلة، لعقد الاتفاقية العربية للأمن السيبراني والدفاع الالكتروني المشترك في مواجهة الحروب والهجمات السيبرانية بمختلف اشكالها، بما يضمن الحفاظ على الحدود الالكترونية والسيادة الالكترونية للدول العربية كافة، والتعاون العربي لضمان الامن في الفضاء السيبراني، والاسترشاد بهذا الشأن بدليل " تالين" للقانون الدولي المنطبق على الحرب السيبرانية .

4- ينبغي على الدول التي تسعى لتطوير قدراتها الدفاعية في نطاق الحرب السيبرانية ان تراعي الحدود الموضوعية لحماية ضحايا النزاعات والحرب السيبرانية من خلال الاعتراف بوجود مستوى جديد من "الحد الادنى الاساسي من الخدمات " التي يجب ان تحظى بالحماية من النزاع السيبراني .

5- ينبغي احداث تعديل جوهري على اتفاقات لاهاي الخاصة بتنظيم وسائل وطرق الحرب من اجل تحريم استخدام القوات غير النظامية في القتال السيبراني وحظر نقل الهجمات السيبرانية عبر شبكات البلدان المحايدة تحت اي ظرف كان .

6- ينبغي تعديل اتفاقيات جنيف لعام 1949 بغرض تحريم الهجمات على البنية التحتية الحيوية التي يمكن ان تعطل الاتصالات الاساسية وتعرض السكان المدنيين للخطر، لاسيما ان تدمير الاتصالات قد يمس الانظمة الصحية ومعالجة المياه وغيرها ...، وهي مجالات ضرورية لبقاء السكان المدنيين احياء، وبالتالي يشملها الحماية وفقا للقانون الدولي الانساني.

7- التزام كل بلد بالا يكون الطرف الذي يبدأ بشن هجوم سيبراني على غيره من الدول الا في الحدود الضيقة والمسموح بها دفاعا عن النفس، منعا لانتشار هذه الهجمات لدول ومنظمات ومجالات يكون من الصعب التحكم في آثارها .

8- التزام كل دولة بالتعاون مع غيرها من الدول ضمن اطار تعاوني دولي لضمان الأمن السيبراني ، وتطوير نظام الامم المتحدة وقوات حفظ السلام من أجل استيعاب مثل هذه الهجمات والحروب السيبرانية في المستقبل.

قائمة المراجع المعتمدة

- **المراجع العربية**

- بن تغري موسى: الحرب السيرانية والقانون الدولي الانساني. مجلة الاجتهاد القضائي. المجلد 12- عدد خاص (العدد التسلسلي 22) أبريل 2020. مختبر أثر الاجتهاد القضائي على حركة التشريع- جامعة محمد خيضر بسكرة- الجزائر.
- ختال هاجر: الوضع القانوني للحرب السيبرانية على ضوء قواعد القانون الدولي. مجلة التواصل في الاقتصاد والإدارة والقانون. جامعة باجي مختار، عنابة، الجزائر. المجلد 25 -العدد 03 - سبتمبر 2019.

- **المراجع الأجنبية**

- ICRC: Cyberwarfare and international humanitarian law: the ICRC's position. 06/2013
- Mary Ellen O'Connell: Cyber Security and International Law. International Law: Meeting Summary. Chatham House. London. 29 May 2012
- Michael N. Schmitt: The law of cyber warfare: Quo Vadis?. Stanford Law & Policy Review. Vol. 25:269. 2014
- Nazanin Baradaran & Homayoun Habibi: Cyber Warfare and Self - Defense from the Perspective of
- International Law. Journal of Politics and Law; Published by Canadian Center of Science and Education. Vol. 10, No. 4; 2017.
- Nils Melzer : Cyberwarfare and International Law. United Nations Institute for Disarmament Research(UNIDIR) RESOURCES. 2011.
- Zain Dar: Cyber Warfare and International Law. Jacobs University Bremen;International Law. Spring 2019.

الأمن السيبراني في الإتفاقية العربية لمكافحة جرائم تقنية المعلومات

الأستاذ خالد اكويس
محام بهيئة المحامين بمراكش (المغرب)

سبق لنا من خلال التقديم المقترح للموضوع ان ثم طرح اشكالية مدى توفق الإتفاقية العربية لمكافحة جرائم تقنية المعلومات , وهو الأمر الذي يقتضي تحليل نصوص هاته الإتفاقية من خلال الجانب الموضوعي ومن خلال الجانب الشكلي كما يلي :

أولا : بنود الاتفاقية من حيث الشكل :

تناولت هذه الاتفاقية العربية مجموعة من المواد من حيث الشكل ويمكن إجمالها في الفصلين الأول والثاني .

1ـ تطرق الفصل الأول في مواده من الأولى حتى الرابعة إلى الحديث عن الهدف من الاتفاقية (المادة1) ثم تحديد المصطلحات (في المادة 2) ثم مجالات تطبيق الاتفاقية (المادة 3) مع الإشارةإلى صون السيادة (المادة 4) .

<u>بحيث انه</u> ، تمت الإشارةإلى أن الهدف من هذه الاتفاقية هو تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لسرد أخطار هذه الجرائم حفاظا على امن هذه الدول ومصالحها وسلامة مجتمعاتها و أفرادها .

ثم تم التطرق إلى التعريف بالمصطلحات المستعملة في هذه الاتفاقية وهي المصطلحات التالية :

1ـ تقنية المعلومات .

2ـ مزود الخدمة .

3ـ البيانات .

4ـ البرنامج المعلوماتي .

5ـ النظام المعلوماتي .

6ـ الشبكة المعلوماتية .

7ـ الموقع .

8ـ الالتقاط .

9ـ معلومات المشترك .

ليتم التطرق في المادة الثالثة إلى مجالات تطبيق هذه الاتفاقية وتمت الإشارةبشأنهاإلى 4 حالات وختم الفصل الأول بالمادة الرابعة التي أشارت إلى ما يسمى بصون السيادة ومبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى بما في ذلك عدم التدخل في ممارسة الولاية القضائية وأداءالوظائف الخاصة بسلطات كل دولة بمقتضى قانونها الداخلي .

2- تطرق الفصل الثاني إلى التجريم وعدد مجموعة من الأفعال التي تلتزم هذه الدول بتجريمها وفقا لتشريعاتها وأنظمتها الداخلية .

وتم تحديد هذه الجرائم فيما يلي :

1 - جريمة الدخول غير المشروع (المادة 6) .

2- جريمة الاعتراض غير المشروع (المادة 7) .

3- الاعتداء على سلامة البيانات (المادة 8) .

4- جريمة إساءة استخدام وسائل تقنية المعلومات(المادة 9) .

5- جريمة التزوير (المادة 10) .

6- جريمة الاحتيال (المادة 11) .

7- جريمة الإباحية (المادة 12) .

8- الجرائم الأخرى المرتبطة بالإباحية(المادة 13) (المقامرة والاستغلال الجنسي) .

9- جريمة الاعتداء على حرمة الحياة الخاصة (المادة 14) .

10- الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات (المادة 15) (محددة في 4 جرائم).

11- الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات (المادة 16) .(محددة في 5 جرائم)

12- الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة (المادة 17) .

13- الاستخدام غير المشروع لأدوات الدفع الالكترونية(المادة 18) .

14 - الشروع والاشتراك في ارتكاب الجرائم (المادة 19) .

15- المسؤولية الجنائية للأشخاص الطبيعية والمعنوية (المادة 20) .

16- تشديد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات (المادة 21) .

ثانيا : بنود الاتفاقية من حيث الموضوع :

تناولت بنود هذه الاتفاقية مجموعة من النصوص من حيث الموضوع وذلك في الفصول الثالث والرابع والخامس.

1ـ **<u>بخصوص الفصل الثالث</u>** (المواد من 22 إلى 29).

تناول الفصل الثالث مجموعة من المعطيات نجملها فيما يلي :

أـالمادة الثانية والعشرون : نطاق تطبيق الأحكامالإجرائية :

تناولت هذه المادة نطاق تطبيق الأحكام الإجرائية وهو ما يخص ضرورة التزام الدول بان تتبنى في قانونها الداخلي التشريعات والإجراءات الضرورية المنصوص عليها في هذه الاتفاقية من خلال تطبيق القانون على:

- ـ الجرائم التي تطرقت لها المادة 6 إلى المادة 19 .
- ـ أية جرائم ترتكب بواسطة تقنية المعلومات .
- ـ جمع الأدلة بشكل الكتروني عن الجرائم .

ب ـ المادتين 23 و 24 :

الملاحظ أن هذه الاتفاقية وان وسعت من نطاق تطبيق الأحكام الإجرامية فقد أعطت أيضا ما سمي بواجب التحفظ شريطة أن يزيد عدد الجرائم التي تطبق عليها الإجراءات المذكورة في المادة 30 وكلما كانت غير قادرة على تطبيقها بسبب محدودية التشريع لديها .

ونلاحظ أن الاتفاقية ميزت بين التحفظ العاجل على البيانات المخزنة في تقنية المعلومات وهو المشار لالتزام الدول بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدارالأمرأو الحصول على الحفظ العاجل للمعلومات المخزنة أو بواسطة إصدارأمرإلى شخص من اجل حفظ معلومات تقنية موجودة بحيازته أولالزام الشخص المسؤول عن حفظ تقنية معلومات للإبقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي .

ثم التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين ، حيث تلتزم كل دولة بتجلي الإجراءات الضرورية في هذا الباب لأجل ضمان توفر الحفظ العاجل لمعلومات تتبع المستخدمين وضمان الكشف العاجل للسلطات المختصة لدى الدولة الطرف حتى يتم تحديد مزودي الخدمة ومسار بث الاتصالات .

ج ـ المواد من 25 إلى 29 :

انه وبعد ضمان السرية في حفظ وصون المعلومات بدأت المادة 25 في الحديث عن أمر تسليم تلك المعلومات سواء بالنسبة إلىالأشخاص الذاتية أو بالنسبة لمزودي تلك الخدمة ثم مسألة ضبط المعلومات المخزنة وتأمينها قصد الوصول إليها وذلك من خلال إجراءات جوهرية تطرقت لها المادة 27 من الاتفاقية .

تم جاءت الاتفاقية انطلاقا من المادة 28 إلى الحديث عن الجمع الفوري لمعلومات تتبع المستخدمين وذلك من خلال تمكين السلطات المختصة من جمع أو تسجيل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف وإلزام مزود الخدمة بان يجمع أو يسجل على إقليم تلك الدولة الطرف ويتعاون ويساعد السلطات المختصة في جمع وتسجيل تلك المعلومات بشكل فوري وذلك في نطاق السرية .

كما تطرقت المادة 29 إلى مجموعة من الإجراءات الجوهرية المتعلقة باعتراض معلومات المحتوى من خلال جمع وتسجيل معلومات المحتوى بشكل فوري والتي تبث بواسطة تقنية المعلومات في إقليم معين ، مع الإشارةإلى انه في حالة عدم استطاعة الدولة الطرف بسبب النظام القانوني الداخلي تبني هذه الإجراءات فيمكنها تبني إجراءاتأخرى بالشكل الضروري لضمان الجمع والتسجيل الفوري للمعلومات في إقليمها .

2ـ بخصوص الفصل الرابع :

لقد تناول الفصل الرابع مجموعة من الإجراءات الخاصة أولابالاختصاص ثم تسليم المجرمين ثم المساعدة المتبادلة والتعاون بخصوص المعلومات العرضية المتلقات وذلك في المواد من 30 إلى 33 .

ليتم التطرق إلى الإجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة في المادة 34 ولرفض المساعدة في المادة 35 ليتحدث عن السرية وحدود الاستخدام والحفظ العاجل للمعلومات المخزنة على أنظمة المعلومات في المادتين 36 و 37 في حين تمت الإشارةإلى التعاون في الكشف العاجل للمعلومات المخزنة والوصول إليها والجمع الفوري وذلك من المواد 38 إلى 43 .

وبشكل مختصر يمكن أن نتحدث عن الاختصاص لما تم الحديث عن تبني الإجراءات الضرورية لهذا الاختصاص في الجرائم المنصوص عليها في هذه الاتفاقية وحددها في تلك التي وقعت إمافي إقليم الدولة الطرف أو على متن سفينة أو طائرة الأولى تحمل علمها الوطني والثانية مسجلة تحت قوانينها .

وبخصوص تسليم المجرمين فان الاتفاقية حددت الحالات والإجراءات الخاصة بتبادل المجرمين بين الدول الأطراف و لتقديم المساعدة في التحقيق بجرائم المعلومات أو لجمع الأدلة الالكترونية في الجرائم في حدود إمكانية رفض هذه المساعدة في حالة اعتبار تلك الجريمة سياسية أو في حالة إمكانية انتهاك لسيادة الدولة أو مصالحها الأساسية حين تنفيذ الطلب .

غير أن هذه الاتفاقية الزمت الدول الأطراف بوجود جهاز متخصص تتحدد مهمته في ضمان توفير المساعدة الفورية لغايات التحقيق وان تكون له القدرة على الاتصالات مع الجهاز المماثل في دولة طرف .

3ـ بخصوص الفصل الخامس :

تطرق الفصل الخامس للأحكام الختامية وذلك من خلال النص على وجوب اتخاذ الإجراءات الداخلية اللازمة لملائمتها مع بنود هذه الاتفاقية وتحديد مسطرة التصديق والإشارةإلى اقتراح التعديلات أو للانسحاب من هذه الاتفاقية.

وتجدر الإشارة الى ان 18 دولة عربية قامت بالتوقيع على هذه الإتفاقية بتاريخ 21 دجنبر 2010 باستثناء سلطنة عمان والتي لم توقع عليها الا بتارخ 15 فبراير 2012 , في حين فإن 8 دول عربية فقط هي من أقرت وصادقت عليها .

ملاحظات حول الإتفاقية

العديد من مواد الاتفاقية تستخدم مصطلحات فضفاضة، سواء كان ما يتعلق بالتجريم أو بجمع البيانات والمعلومات عن المستخدمين أو حتى في المبادئ العامة التي استندت عليها، وبالتالي فإن موادها القانونية ستؤثر سلباً على مجموعة من الحقوق والحريات والتي تتصل بحرية التعبير والحق في الخصوصية .

مبدأ وضوح النص القانوني هو حق أصيل للناس، فلا يجب أن تحتوي نصوص الاتفاقية على ألفاظ غير مُحكمة وغير مُحددة .فمواد الاتفاقية تحتوي على العديد من الألفاظ والعبارات الفضفاضة والغير مُحددة يقيناً وتحتمل التأويل في جوانبها .وكان على الاتفاقية أن تستخدم ألفاظ واضحة الدلالة والتأويل والتفسير وأن لا يُترك تفسيرها وتأويلها إلى للأجهزة القضائية والتنفيذية بالدول أطراف الاتفاقية، بل أنه من المفترض أن يقتصر دور أجهزة تطبيق القانون على التحقق والتأكد من ارتكاب الجرم من عدمه.

أولا : نصوص غامضة ومصطلحات فضفاضة :

.على سبيل المثال في المادة 9، تُجرِّم إساءة استخدام وسائل تقنية المعلومات، حيث تعتبر الاتفاقية أن إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في

المادة السادسة إلى المادة الثامنة هذا التجريم واسع جداً، ويمكنه أن يشمل العديد من التطبيقات والبرمجيات التي يتم استخدامها في اختبارات أمن وحماية الشبكات والبرمجيات والأنظمة المعلوماتية وتستخدم بالأساس لكشف الثغرات الأمنية للأنظمة وشبكات الاتصالات والبرمجيات ، ما يعني أن حيازة هذه التطبيقات أو برمجتها يُعتبر جريمة، وهو ما يعكس عدم تناسب المادة مع واقع المعطيات التقنية فيما يتعلق بالأمن الرقمي.

وفي المادة 12 تتناول جريمة الإباحية حيث تُشدد العقوبة في الجرائم المتعلقة بإباحية الأطفال والقاصرين ويشمل هذا التشديد حيازة مواد إباحية الأطفال والقصر أو مخلة بالحياء للأطفال والقصر على تقنية المعلومات أو وسيط تخزين

تلك التقنيات، ورغم أهمية هذه المادة وتناسبها مع المعايير الحقوقية والأعراف الإنسانية والمواثيق الدولية، إلا أنها تترك باباً مفتوحاً أمام الحكومات العربية لتفسيرها طبقا لمعايير غير معروفة وليست مُحددة في الاتفاقية ولا يوجد أي تعريف واضح لماهية المواد المخلة بالحياء وعليه فإنه يمكن استخدامها فعليا لتجريم العديد من أنواع المحتوى المنشور على الإنترنت سواء كانت نصوصاً أدبية أو أعمال فنية أو أي من أنشطة النشر على الرقمي، خاصة أن هذه الألفاظ الفضفاضة استُخدمت سابقا بالفعل لتقييد حرية التعبير وتجريم أعمال أدبية وفنية .

وفي المادة 15 حيث تتناول الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، وتنص في النقطة الرابعة منها على تجريم نشر النعرات والفتن والاعتداء على الأديان والمعتقدات . هذه المادة يمكن استخدامها لتجريم أي رأي أو تعبير يمكنه أن يُشكّل اختلافا مع المعتقدات الدينية والاجتماعية السائدة .في أي من الدول الأعضاء مثلاً هناك العديد من القضايا المتعلقة بازدراء الأديان وضحايا حُكموا بسبب تعبيرهم عن معتقداتهم واعتبار آرائهم اتجاه الدين كنوع من أنواع الاعتداء على الأديان، سواء كان ذلك برأي مباشر اتجاه معتقدات دينية أو من خلال أعمال فنية وأدبية .

ثانياً : أحكام إجرائية تنتهك سرية البيانات والحق الخصوصية

لم تنص الاتفاقية بشكل واضح على مواد من شأنها أن تُحافظ على خصوصية المُستخدمين وبياناتهم وحقوقهم بل على العكس، احتوى فصل الإجراءات على نصوص عديدة لا تُراعي أي مبادئ أو معايير حقوقية في الجمع أو الاحتفاظ بالبيانات .وكان المفترض أن يكون صيانة الحقوق والحريات واحدة المبادئ التي تُعتَمَد في صياغة الاتفاقية، خاصة ما يتعلق بالحق في الخصوصية وسرية البيانات الشخصية وحرية التعبير، وعدم ترك مساحة للتفسيرات والتأويل القانوني بالشكل الذي يوفّر القدر الأقصى من حماية الحقوق والحريات، ووضع حدود قانونية للجمع والاحتفاظ بالبيانات .

على سبيل المثال المادة 23 من الاتفاقية تُلزم كل دولة بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة، وتذكر المادة بما في ذلك معلومات تتبع المستخدمين ولم تضع المادة أي ضوابط قانونية للحصول على هذه المعلومات (كاستصدار أمر قضائي بذلك) وأيضا لم تضع حدا للمدة الزمنية التي يجب أن يتم الاحتفاظ بها بالبيانات بل نصت على أن هذه البيانات يُحتفظ بها عن طريق شخص مسؤول بحفظها وصيانة سلامتها لمدة أقصاها 90 يوما قابلة للتجديد ولم يتم تحديد مرات التجديد أو شروطه أو إجراءاته أو مدى ضرورته في أي من بنود الاتفاقية.

وهذا ما تسير عليه المادة 28 أيضاً والتي تتناول الجمع الفوري لمعلومات تتبع المستخدمين وتُلزم الدول بتبني الإجراءات الضرورية لتمكين السلطات المختصة من جمع أو تسجيل المعلومات، وتُعطي للحكومات إمكانية" تبني

إجراءات أخرى بالشكل الضروري لضمان الجمع أو التسجيل الفوري لمعلومات تتبع المستخدمين المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية ولم تذكر المادة أي حدود أو ضوابط قانونية للجمع الفوري للمعلومات، فقط تم إلزام الدولة بالحفاظ على سرية المعلومات دون وجود أي إشارة لمدة الاحتفاظ بالمعلومات .

ثم تأتي المادة 29 وتتوسع في إجازة تبني إجراءات لم تُذكر في الاتفاقية لجمع وتسجيل المعلومات، إذا لم تستطع الدولة الطرف بسبب نظامها القانوني الداخلي من اتخاذ إجراءات الجمع والتسجيل للمعلومات، المُعترَضة، وأشرت المادة لهذه الإجراءات بجملة تبني إجراءات أخرى دون أي تحديد لضوابط قانونية وحدود حقوقية.

وفي المادتين 24 و 25 والتي تُلزم الدول بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص "أو" أي مزود خدمة بتسليم المعلومات، دون تحديد أي ضوابط قانونية ضرورية لوضع حدود ملائمة ومناسبة من شأنها أن تحمي الحق في الخصوصية وحماية المعلومات الشخصية .وعلى نفس المنوال تسير المادة 28 والتي تتناول" ضبط المعلومات المخزنة "حيث تُلزم المادة في فقرتها الثانية كل دولة أن تتبنى الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات لتقديم المعلومات الضرورية لإتمام إجراءات نسخ معلومات تقنية المعلومات والاحتفاظ بها والحفاظ على سلامتها وإزالة أو منع الوصول لها، ما يعني أن المادة تُجيز للسلطات المختصة الاستعانة بعناصر من خارج القطاعات الحكومية وهو ما يُشكّل انتهاكا لخصوصية المواطنين.

ثالثاً : مشاركة البيانات بين الدول الأطراف والخصوصية

الفصل الرابع من الاتفاقية يُنظم التعاون القانوني والقضائي بين الدول أطراف الاتفاقية، واستمراراً لاستخدام المُصطلحات الغير مُحكمة والفضفاضة فقد تم استخدام مصطلحي" المصالح العليا للدولة "و"الجرائم السياسية "وهي فعليا لم يتم وضع تعريف واضح لها ضمن الوثيقة، كما أن الفصل لم يشترط على ضرورة حماية البيانات في حالة مشاركة البيانات بين الدول.

في المادة 30 تُلزم الاتفاقية كل دولة بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني(فصل الجرائم) وذلك إذا ارتكبت الجريمة وكانت تمس أحد المصالح العليا للدولة و فعلياً لم يتم تحديد ماهية" المصالح العليا للدولة "وهو مصطلح سيئ السمعة ان صح التعبير و كثيراً ما يستخدم ضد نشطاء الإنترنت والساعين لإحداث تغيرات اجتماعية وسياسية، ما يعطي الدول الأعضاء صلاحية لتفسيره طبقا لرؤيتهم أو مصالحهم والتي ربما يروا فيها" المصالح العليا للدولة."

وتتناول المادة 33 المعلومات العرضية المتلقاة والتي تُجيز للدولة مشاركة المعلومات التي تم الحصول عليها من خلال تحقيقاتها مع دول أخرى، دون طلب مسبق، إذا كانت هذه المعلومات يمكن أن تساعد الدولة الطرف المرسلة إليها في إجراء الشروع أو القيام بتحقيقات في الجرائم المنصوص عليها في هذه الاتفاقية وتُجيز الفقرة الثانية من نفس المادة للدولة المزودة بالمعلومات أن تطلب الحفاظ على سرية المعلومات، وإذا لم تستطع الدولة الطرف المستقبلة الالتزام بهذا الطلب يجب عليها إبلاغ الدولة الطرف المزودة بذلك والتي تقرر بدورها مدى إمكانية التزويد بالمعلومات ، فالنص يُجيز مشاركة المعلومات دون اشتراط السرية، بل تُرك الموضوع اختياريا للدولة المزودة بالمعلومات ولم يتم تحديد ما إذا كانت معلومات شخصية أم لا .وكان على الاتفاقية أن تُلزم الطرفين بسرية المعلومات في حالة أن كانت تحتوي أي معلومات أو بيانات شخصية ومنع تشارك المعلومات مع دول لا تلتزم بمعايير واضحة للسرية.وهذا ما تسير عليه أيضا المادة36 .

وتناولت المادة37 الحفظ العاجل للمعلومات المخزنة على أنظمة المعلومات وأعطت الحق لأي دولة طرف أن تطلب من أي دولة طرف أخرى الحصول على الحفظ العاجل للمعلومات المخزنة على تقنية المعلومات تقع ضمن إقليمها بخصوص ما تود الدولة الطرف الطالبة للمساعدة أن تقدم طلبا بشأنه للمساعدة المتبادلة للبحث وضبط وتأمين وكشف المعلومات ثم نصت المادة في فقرتها السادسة على أن أي حفظ يجب أن يكون لفترة لا تقل عن (60) يوما من أجل تمكين الدولة الطرف الطالبة من تسليم البحث أو الوصول أو الضبط أو التأمين أو الكشف للمعلومات . وبعد استلام مثل هذا الطلب يجب الاستمرار بحفظ المعلومات حسب القرار الخاص بالطلب و مرة أخرى لا تذكر الاتفاقية بشكل واضح مدة حفظ المعلومات، بل ألزمت الدول بالاستمرار في الحفظ دون تحديد لأي مدة ولا اشتراطات واضحة لمد مدة الحفظ.

وعلى نفس شاكلة استخدام مصطلحات غير مُعرّفة بشكل واضح في الاتفاقية، فقد أجازت المواد 35 و36 و38 للدول الأطراف رفض أو تعليق الاستجابة لمشاركة المعلومات مع دول أخرى إذا كانت تتعلق بجريمة تُعتبر جريمة سياسية أو انتهاكات لمصالحة الأساسية ولم يتم تعريف الجريمة السياسية في أي من بنود الوثيقة تماما.

الخلاصة

أن الاتفاقية تحتوي على العديد من الثغرات التي يمكن استخدامها للتضييق على حرية الرأي والتعبير والحق في الخصوصية على الإنترنت، وبشكل عام يمكن أن يتم تلخيص مُجمل التحفظات على الاتفاقية كالآتي:

- استخدمت الاتفاقية مجموعة من المصطلحات والألفاظ، تم تكرارها في أكثر من موضوع، دون وجود تعريف مُحكم ومنضبط لها في أي مكان بالاتفاقية.
- لم يتم وضع قواعد قانونية مُحددة على الإجراءات المتبعة لجمع البيانات والمعلومات في فصل الإجراءات.

- لم يتم النص بشكل مباشر في الإتفاقية على مبادئ من شأنها أن تضع حدودا بحيث لا يتم تطبيق بنود الوثيقة بالشكل والطريقة التي تحد من حرية التعبير أو تنتهك الحق في الخصوصية.
- بنود الاتفاقية لم تراعي تناسب التجريم مع التطور التكنولوجي في مجال الاتصالات وتكنولوجيا المعلومات.

توصيات :

- توصية 1 : يجب تقديم طلب للإعادة صياغة بعض المصطلحات بالإتفاقية مع اعطاء تعاريف محكمة لمجموعة من التعابير بشكل واضح ودقيق منعا لأي تأويل .
- توصية 2 : يجب الإشارة لمأل مجموعة من الأجالات المضمنة بالإتفاقية في حالة فوات المدة دون القيام بالمطلوب احتراما للحق في الخصوصية وضمانا لكل محاكمة عادلة .
- توصية 3 : فتح الباب أمام الدول الأعضاء لتقديم مقترحات جديدة لها علاقة بالتطور التكنولوجي في مجال الإتصالات وتكنولوجيا المعلومات .
- توصية 4 : يجب أن يتم اضافة دول عربية أخرى للإتفاقية أو اقناع بعضها بالمصادقة حتى تعمم ويتحقق التبادل والتعاون في محاربة الجرائم العابرة للقارات .

الامن السيبراني و سلامة المعطيات
ذات الطابع الشخصي على ضوء قانون 08.09

الأستاذة زهرة خلوق
محامية بهيئة المحامين بمراكش (المغرب)

يعتبر أمن البيانات الشخصية المنشأة على دعامة إلكترونية جزء لا يتجزأ مما يعرف بالأمن السيبراني الذي يعنى بأمن الحاسوب أو أمن المعلومات والتي من بينها البيانات المؤسسة للمعطيات الشخصية للأفراد ذلك أن لكل شخص حق دستوري في حماية حياته الخاصة طبقا لمقتضيات لفصل 24 من الدستور المغربي[248] .

وعليه فإنه يمنع معالجة المعطيات الشخصية للأفراد أو الحصول عليها إلا استثناء كما هو منصوص عليه في الفصل 27 من الدستور المغربي[249] . ولكون المشرع المغربي جرم كل الأفعال الهادفة إلى الوصول أو التلاعب أو الحصول على المعطيات الشخصية للأفراد بقصد الإساءة إلى أصحابها أو ابتزازهم، فقد أعتبر الأمن السيبراني بهذا الخصوص أهم مستند قانوني يمكن أن يحقق الحماية اللازمة لهذه المعطيات انسجاما مع مقتضيات قانون 08.09 المتعلق بحماية المعطيات ذات الطابع الشخصي.

وللأمن السيبراني عدة أجهزة وآليات تتجه نحو إيجاد السبل الكفيلة لرد الهجوم الالكتروني و أخص بالذكر الهجوم على المعطيات ذات الطابع الشخصي وهي إما آليات تشريعية أو أمنية وإما آليات قضائية وهي الاليات التي سنعمل الى التطرق اليها بصدد هذا البحث قصد الاجابة على اشكال الموضوع المتمثل في:

مدى فعالية الامن السيبراني في حماية المعطيات الشخصية من خلال قانون 08.09 ؟ .

وكذا الاسئلة المتفرعة عنه والمتمثلة في مدى نجاعة قانون الامن السيبراني وكذا قانون حماية المعطيات الشخصية في حماية المعطيات الشخصية للأفراد؟ ثم ما العلاقة بين قانون 05.20 وقانون 08.09؟

---

248 ينص الفصل الأول من الدستور المغربي على ما يلي : " لكل شخص الحق في حماية حياته الخاصة".

249 ينص الفصل الثاني من الدستور المغربي على ما يلي: " ... لا يمكن تقييد الحق في المعلومة الا بمقتضى القانون بهدف حماية كل ما يتعلق بالدفاع الوطني وحماية امن الدولة الداخلي والخارجي والحياة الخاصة للافراد وكذا الوقاية من المس بالحريات والحقوق الأساسية المنصوص عليها في هذا الدستور...".

وذلك من خلال تقسيم الموضوع الى محورين اساسيين يتضمن **المحور الاول** المظاهر الحمائية للأمن السيبراني وعلاقته بقانون 08.09 في حين يتضمن **المحور الثاني** اهم الاليات الحمائية للأمن السيبراني في حماية المعطيات ذات الطابع الشخصي.

المحور الأول: المظاهر الحمائية للأمن السيبراني للمعطيات ذات الطابع الشخصي على ضوء قانون 08.09

تهم حماية المعطيان الشخصية كل ما يتعلق بالحياة الشخصية للافراد من بياناته واتصلاته ومواصلاته وعلاقاته الشخصية التي تندرج في اطار الحياة الشخصية له كفرد من افراد المجتمع والتي لا يحق للغير معرفتها او الوصول اليها الا عن طريقه او باذنه، وعليه فان كل محاولة للحصول على هذه المعلومات يعتبر جرما يستوجب العقاب كون الحياة الخاصة تعتبر حرمة محظور الاعتداء عليها. ولذلك كان لازما على المشرع ان يصدر قوانين من شانها ان تكفل هذه الحماية استجابة للتطورات التشريعية التي تعرفها حماية الحياة الخاصة للافراد من الهجمات الالكترونية على الخصوص

وهو ما اسفر عن اصدار عدة قوانين بشأن الموضوع عبر خط زمني متدرج لتغطية الجرائم الماسة بالمعطيات الشخصية للافراد **(الفقرة الاولى)** وصولا الى اصدار قانون 05.20 المتعلق بالامن السيبراني الذي يعتبر المرجع الاساس في هذا النوع من الجرائم بدء من دخوله حيز التطبيق **(الفقرة الثانية)**.

الفقرة الاولى: التطور التاريخي للتشريع المغربي في مجال الأمن السيبراني الخاص بالمعطيات الشخصية ونشأته.

من المعلوم أن القوانين ليست وليدة اللحظة وإنما هي تراكمات للعديد من التشريعات والمراسيم والنصوص المتفرقة التي تؤدي في نهاية المطاف إلى إيجاد قانون إطار يجمع شتات التشريع فيما يخص ظاهرة جديدة كما هو الشأن بالنسبة للأمن السيبراني، هذا الأخير الذي عرف جدولا زمنيا كانت بدايته ما قبل سنة 2000 وذلك بسن القانون رقم 24.96 المتعلق بالبريد والاتصالات لسنة 1998.

و ليكون بعد ذلك أول قانون يدخل في اطار الامن السيبراني هو القانون رقم 07.03 المتمم للقانون الجنائي والمتعلق بالجرائم المتعلقة بالمعالجة الالية للمعطيات الصادر سنة 2003[250] ليعقبه بعد ذلك القانون رقم

[250] وللاشارة فقد سبق للقضاء ان بت في مثل هذه القضايا كما هو الشأن لحكم المحكمة الابتدائية بالبيضاء بين السيد وكيل الملك والصحفيان نور الدين مفتاح ومريم مكريم عن جريدة الايام التي قامت بنشر مقال تحت عنوان (ثورة الحريم بين ثلاثة
=

53.05 المتعلق بالتبادل الالكتروني للمعطيات القانونيـــة والصادر سنة 2007 وصولا إلى القانون 08.09 المتعلق بحماية الأشخاص الذاتيين اتجاه معالجة المعطيات ذات الطابع الشخصي، هذا الأخير الذي يعد أحد الأجهزة أو الآليات التي ينهض عليها الأمن السيبراني فيما يخص المس بالمعطـــيات ذات الطابع الشخصي، تم أخيرا صدر قانون 05.20 المتعلق بالأمن السيبراني الذي فرضه التطور التكنولوجي الذي عرفه العالم بصفة عامة .

هذا الاخير الذي أنشأ من اجل تعزيز امن نظم المعلومات سواء في ادارات الدولة ومؤسساتها او في المقاولات العمومية والمقاولات التجارية والشركات التجارية خاصة المتعقلة بمجال الخدمات وبصفة عامة كل شخص يدخل في إطار القانون العام او القانون الخاص والذي يتعلق مجال عملهم بقطاع الخدمات التي تستلزم معالجة المعطيات ذات الطابع الشخصي.

الفقرة الثانية: المظاهر الحمائية للمعطيات الشخصية على ضوء قانون 05.20

اولا: قانون 05.20 المتعلق بالامن السيبراني[251] .

أعد قانون 05.20 من طرف ادارة الدفاع الوطني مع احداث مجموعة من الاجهزة التي تعنى بمهمة الدفاع والامن المعلوماتي من بينها المجلس الوطني للأمن السيبراني والمركز الوطني للأمن السيبراني بشخصية اعتبارية ذات استقلال مالي و إداري هدفهما الأساسي حماية الامن الاقتصادي والقومي والمنظومة المعلوماتية بصفة عامة على رأسها حماية الحياة الخاصة للأشخاص.

كما يهم الامر احداث لجنة استراتيجية للأمن السيبراني ولجنة تابعة لها لإدارة الازمات والاحداث السيبرانية الجسيمة ثم السلطة الوطنية للأمن السيبراني بما يشكل هيئات متكاملة فيما بينها من أجل رد الهجمات الامنية الالكترونية. وبالرجوع إلى المادة 2 من قانون 05.20 نجد ان المشـرع عرف الأمن السيبراني بكونه مجموعة من التدابير والإجراءات ومفاهيم الأمن وطرق إدارة المخاطر والأعمال والتكويـــنات وأفضل الممارسات والتكنولوجيات التي تسمح لنظام معلومات أن يقاوم أحداثا مرتبطة بالفضاء السيبراني من شأنها أن

ملوك) يهم معلومات على أساس انها الحياة الخاصة للقصر الملكي ونشر صور الاسرة الملكية دون الحصول على اذن من الديوان الملكي الامر الذي قضت على اثره المحكمة باذانة التهمان بالمنسوب اليهما بأربعة اشهر حبسا موقوف التنفيذ.

حكم عدد: 06/5141 بتاريخ 13/02/06 ملف جنحي رقم: 2006/153 منشور بمجلة المنبر القانوني العدد 9 سنة 2015 ص 42 وما يليها.

[251] ظهير شريف رقم 1.20.96 صادر في 4 ذي الحجة 1441 (25يوليوز 2020) بتنفيذ القانون رقم 05.20 المتعلق بالامن السيبراني المنشور بالجريدة الرسمية عدد 6904-9 ذو الحجة 1441 (30 يوليوز 2020).

تمس بتوافر وسلامة وسرية المعطيات المخزنة أو المعالجة أو المرسلة والخدمات ذات الصلة التي يقدمها هذا النظام أو تسمح بالولوج إليه.

من هذا التعريف نجد أن المشرع المغربي استعمل مجموعة من المصطلحات الفضفاضة والشاسعة والتي يمكن ان تقبل أكثر من معنى، بمعنى ان التعريف الذي اتى به المشرع المغربي وبالرغم من غموضه فهو تعريف مرن بإمكانه الاستجابة لما قد يأتي من مظاهر مستحدثة في مجال الاجرام الالكتروني.

وانطلاقا من القراءة الأولية للتعريف الذي أعطاه المشرع المغربي للأمن السيبراني نجد أن هذا الأمن يتحقق عبر هيئات تسهر على ذلك كل بحسب اختصاصها والتي لها الحق أن تتخذ كل الإجراءات التقنية والتنظيمية لمواجهة مخاطر الفضاء السيبراني. ويجب على كل هيئة وبحسب المادة 5 [252]من القانون 05.20 أن تحدد إجراءات تأهيل الأشخاص الذين يمكنهم الولوج إلى المعلومات المصنفة وشروط معالجة هذه المعلومات أو تبادلها أو تخزينها أو نقلها مع العلم أن هذا القانون لا يهم فقط المعلومات المصنفة وإنما حتى المعطيات الشخصية،

هذه الأخيرة التي أثارت نقاش حول ماهيتها وهل تشمل الصوت و الصور الخاصة بالأفراد؟

ثانيا: قانون 08.09 المتعلق بحماية المعطيات ذات الطابع الشخصي[253]

سبق القول سلفا ان قانون 08.09 يعتبر جزء لا يتجزأ من قانون 05.20 المتعلق بالأمن السيبراني ذلك ان امن المعطيات الشخصية جزء من الامن المعلوماتي بصفة عامة وسلامتها يدخل في اولويات الامن السيبراني وعليه فقد خص لأمن المعطيات الشخصية قانونا خاصا به قانون 08.09 جاء سابقا على قانون الامن السيبراني هذا الاخير الذي يعتبر الاطار العام لهذه الحماية، وتبدوا اهمية هذا القانون في كونه سيساهم في تقوية ثقة

---

[252] تنص المادة 5 من قانون 20.05 على ما يلي: يجب على كل هيئة ان تقوم بتصنيف أصولها المعلوماتية ونظم معلوماتها حسب مستوى حساسيتها من حيث السرية والتمامية والتوافر. كما يتعين ان تكون تداتبير حماية الأصول المعلوماتية ونظم المعلومات متناسبة مع مستوى التصنيف المخصص لها.

يجب على كل هيئة ان تحدد إجراءات تاهيل الأشخاص الذين يمكنهم الولوج الى المعلومات المصنفة وشروط معالجة هذه المعلومات او تبادلها او تخزينها او نقلها.

يحدد بنص تنظيمي الدليل المرجعي لتصنيف أصول المعلومات ونظم المعلومات".

[253] الظهير الشريف رقم 1.09.15 صادر في 22 من صفر 1430 (18 فبراير 2009) بتنفيذ القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي الجريدة الرسمية عدد 5711 بتاريخ 27 صفر 1430 (23 فبراير 2009).

المستهلك المغربي في مجال المعلوميات و المعاملة الالكترونية وتتجلى اهمية موضوع حماية المعطيات ذات الطابع الشخصي في رصد مدى تأثير الواقع المعلوماتي الجديد على الحق في الخصوصية ؟.

حمايةالمعطيات ذات الطابع الشخصي لاتعني الحد من تداولها كما جاء على لسان رئيس اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي بل تعني تقنين معالجتها بما يحفظ مصالح المواطنين وحقوقهم، خاصة وان جل دول العالم تتجه الى رقمنة المعطيات الشخصية للأفراد بكل جوانبها من صحية واقتصادية وعدلية وامنية لما سيساعد ذلك في سهولة وسرعة تقديم الخدمات الادارية للمواطنين بشكل امن وهو ما قد يفسر ما تعرفه كل ادارات المغرب من رقمنة اجراءاتها فنجد المحكمة الرقمية وتعديل قانون الحالة المدنية وتمكين المواطنين من الحصول على وثائقهم الادارية بشكل الكتروني يقصر المسافات والزمن للحصول عليها وهذا ما يستوجب احداث فضاء الكتروني يعالج هذه المعطيات بشكل امن والامن هنا يتحقق عن طريق الامن السيبراني.

ويهدف قانون 08.09 الى فرض اجراءات قانونية صارمة ضد اساءة استخدام هذه البيانات وأحدث لذلك اللجنة الوطنية لمراقبة المعطيات ذات الطابع الشخصي والسهر على تنفيذ مقتضيات هذا القانون[254]، كما احدثت المديرية العامة لأمن المعلومات255 و التي تعد الهيئة المسؤولة عن امن الانترنت بالمغرب.

ويمكن تعريف المعطيات الشخصية بكونها كل معلومة من شانها ان تعرف بشخص طبيعي او تسهل ذلك اما بصفة مباشرة او غير مباشرة256وما يدخل في اطارها الصوت والصورة.

كما عرفها المشرع بمقتضى المادة 1/1 من قانون 08.09 "**بكونها كل معلومة كيفما كان نوعها بغض النظر عن دعامتها بما في ذلك الصوت والصورة والمتعلقة بشخص ذاتي معرف او قابل للتعرف عليه**

---

[254] تتشكل هذه اللجنة من شخصيات ذات مستوى عال من النزاهة والكفاءة في المجال القانوني والقضائي والمعلوماتي وتتكون من رئيس يعينه الملك وستة أعضاء يعينهم الملك بناء على اقتراح من الوزير الأول ورئيس مجلس النواب ورئيس مجلس المستشارين بنسبة لعضوين لكل واحد منهم . تاسسست بتاريخ 18 فبراير 2009 بمقرها الرئيس الرباط

موقعها الرسمي http://www.cndp.ma من بين اهم اختصاصاتها الى جانب الاستشارة والاقتراح معالجة الشكايات والتحري والمراقبة.

[255] حنان اسويكت، الحماية الجنائية للمعطيات ذات الطابع الشخصي على ضوء القانون 08.09، مجلة العلوم الجنائية العدد الرابع سنة 2017 ص 246.

[256] حنان اسويكت م س ص 246. وما يليها

والمسمى بعده "الشخص المعني" ويكون الشخص قابلا للتعرف عليه اذا كان بالإمكان التعرف عليه بصفة مباشرة او غير مباشرة ولاسيما من خلال الرجوع الى رقم تعريف او عنصر او عدة عناصر مميزة لهويته البدنية او الفيزيولوجية او الجينية او النفسية او الاقتصادية او الثقافية او الاجتماعية"

ومن خلال هذا التعريف نجد انه جاء شاملا لكل ما يمكن ان يدخل في إطار التعريف بالأشخاص وتحديد هويتهم الامر الذي يجعل مصطلح المعطيات الشخصية مصطلحا شاملا سيمكن فيما بعد من استقطاب عناصر اخرى تدخل في إطار المعطيات الشخصية ولعل هذا من حسنات التعريف الواسع الذي تبناه المشرع المغربي.

المحور الثاني: المقاربة الأمنية والزجرية للأمن السيبراني في حماية المعطيات ذات الطابع الشخصي:

ان مجرد المس بالمعلومات الشخصية داخل الفضاء الالكتروني يعتبر جريمة الكترونية بل ان اقتحام المجال الالكتروني والبقاء فيه يعبر جريمة معاقب عليها[257] ناهيك عن معالجة هذه المعطيات والاضرار بأصحابها.

ومن المعلوم ان معطيات الافراد معرضة في أي زمان ومكان للقرصنة وللمعالجة بل وللتحايل واستعمالها في ارتكاب جرائم ومثل هذه القضايا ليست غريبة على القضاء وعلى اهل الاختصاص.

وعليه فان احداث الاجهزة الامنية الكفيلة بتتبع المخترقين للمعطيات الشخصية وارتكاب الجرائم خاصة الجرائم الالكترونية منها كان لازما **(الفقرة الاولى)** وهو ما سيمكن القضاء في انصاف المتضررين ممن استغلت معطياتهم ومعلوماتهم الشخصية في ارتكاب هذه الجرائم و الاضرار بهم ماديا ومعنويا **(الفقرة الثانية).**

الفقرةالاولى: المقاربة الأمنية لحماية المعطيات ذات الطابع الشخصي:

وتهم أساسا الأجهزة الامنية المستحدثة من طرف المشرع في هذا الخصوص والتي تهدف بالأساس الى الوصول الى المعالجين للمعطيات الشخصية سواء كانوا اشخاصا طبعيين او اشخاصا معنويين بما فيهم السلطة العامة، حيث ان المعالجة بحد ذاتها التي تدخل في إطار تنظيمي أو صحي أو اداري أو حتى تربوي لا تعتبر بحد ذاتها جرما وانما المعالجة بطريقة مغلوطة او غير امنة و التي سهلت للغير من قراصنة الانترنيت الوصول اليها والاساءة الى اصحابها هي التي تعتبر جرما تصدى لها القضاء في العديد من احكامه وايدته محكمة النقض والتي جاء في حيثياتها " حيث ان القرار المطعون فيه سالم من كل عيب شكلي وان الاحداث التي

[257] صليحة حاجي، الاليات القانونية لتكريس الامن المعلوماتي، مقال منشور بمجلة العلوم الجنائية العدد الثاني سنة 2015 ص 9 وما يليها.

صرحت امحكمة بثبوتها بما لها من سلطان ينطبق عليها الوصف القانوني المأخوذ به كما انها تبرر العقوبة المحكوم بها" [258]، و تهدف كذلك هذه الهيئات الوصول الى المعالجين ممن ليس لهم الحق في اخذ واستعمال المعطيات الشخصية للأفراد ومعالجتها الكترونيا او توظيفها في انشاء مواقع بقصد الابتزاز او بقصد الاختراق الامني لمؤسسة ما، سواء تواجد هؤلاء المعالجين على ارض المغرب او خارجه، وهنا يطرح اشكال تنازع الاختصاص .

وكما تم إحداث مختبر للتحليل الجنائي للجرائم المتعلقة بالمعالجة الآلية للمعطيات الشخصية سنة 2003 **وكذا اللجنة الوطنية لمراقبة وحماية المعطيات ذات الطابع الشخصي** والتي تعنى بتنفيذ مقتضيات قانون 08.09 وتعنى كذلك بتلقي شكايات المتعلقة بالمس بالمعطيات الشخصية ،والاشكال المطروح في هذا الصدد على المستوى العملي : هل هذه اللجنة الوطنية المعنية بحماية المعطيات ذات الطابع الشخصي تقوم فعلا بالمهام المنوطة بها و هل لها تنسيق مع النيابة العامة كجهة مختصة في تحريك الدعاوى العمومية وهل المواطن كمستهلك للتكنولوجيا على علم بوجود هذه اللجنة من الأساس.

وفي نفس السياق وفي إطار التحديث وإنشاء الآليات الكفيلة للحد من مخاطر الفضاء السيبراني انخرط المغرب في مسار التوعية والتحسيس بمخاطر الجرائم الالكترونية وتكوين خبراء متخصصين في مجال الرصد والتحليل في مجال الأمن السيبراني والانضمام إلى دورات تكوينية أطر العدالة في مجال الأمن ونظم المعلومات .

الفقرة الثانية : المقاربة الزجرية والقضائية

نقصد بالمقاربة الزجرية تلك المقتضيات القانونية التي نص عليها المشرع بمقتضى القانون الجنائي أو قانون 08.09 وكذا قانون 05.20 المتعلق بالأمن السيبراني والتي تنصب في جزر المخالفات والجرائم التي تمس المعطيات الشخصية.

أولا: على مستوى العقوبـــة:

فعلى مستوى القانون الجنائي نجد المشرع المغربي نص على تجريم كل فعل وتغريمه كلما كان الغرض من هذا الفعل المس بالمعطيات الشخصية للأفراد كما هو منصوص عليه بمقتضى الباب العاشرمن القانون

---

[258] **وتهم الجرائم المتابع من اجلها المتهمون بالمس بنظم المعالجة الالية للمعطيات حيث تمت الادانة بثلاث سنوات حبسا نافذا . قرار غرفة الجنايات الاستئنافية بمحكمة استئناف تطوان، الصادر بتاريخ 2012/2/8 تحت عدد 2012/92 في القضية الجنائية عدد 2011/575 منشور بكتاب الجرائم المعلوماتية في ضوء التشريع والقضاء المغربي واليمني عز الدين بن امية الاموي، مكتبية دار السلام الطبعة الاولى 2021ص 93 وما ييليها.**

الجنائي تحت عنوان المس بنظم المعالجة الالية للمعطيات والذي جاء بأقصى عقوبة سجنية يمكن أن يحكم بها هي 5 سنوات حبسا.

كما أنه من الملاحظ على ان المشرع المغربي استعمل مصطلح حبسا وليس سجنا الامر الذي يوضح أن المشرع لم يعطي لهذه الجرائم صفة الجناية رغم خطورتها واحتفظ بوصفها كجنحة فقط.

اما على مستوى قانون 08.09 فان اقصى عقوبة حبسية حددها المشرع هي سنتين حبسا وغرامة لاتتجاوز مبلغ 300.000 درهم، مما تكون هذه العقوبات لا تحقق لا الردع العام ولا الخاص بخصوص الجرائم الالكترونية.

وفيما يهم المقتضيات الزجرية التي جاء بها القانون 05.20 المتعلق بالأمن السيبراني فمن خلال استقرائنا لمقتضيات هذا القانون نلاحظ انه لم يأتي بالعقوبات الحبسية سواء النافذة او الموقوفة وانما جاء بعقوبات على شكل غرامات مرتفعة وعيا منه ان العقوبة السالبة الحرية لم تعد تحقق الردع العام ولا الخاص، مع ملاحظة ان المشرع المغربي من خلال سنه للقانون المتعلق بالأمن السيبراني اهتم بالجاني الشخص المعنوي أكثر من الشخص الذاتي.

ثانيا: على مستوى العمل القضائي

نظرا لخطورة الجرائم الالكترونية بصفة عامة و الماسة بالمعطيات الشخصية بصفة خاصة فالقضاء المغربي كان دائم التصدي لمثل هذه الجرائم التي تهم المس بالمعطيات ذات الطابع الشخصي فنجده يقضي إما بالتعويض أو الإدانة لمن تضرر من هذه الجرائم وكمثال على ذلك قضت محكمة النقض في قرار لها عدد 372/1 بما يلي: **(أي زبون لأي بنك تم اختراق أو قرصنة القن السري لبطاقته البنكية فمن حقه رفع دعوى التعويض ضد البنك المعني بالأمر لأنه يعد مسؤولا عن عدم توفره على نظم معلوماتية مؤمنة ضد جرائم الاختراق وقرصنة القن السري)** هذا قرار صادر بتاريخ 2017/07/27 في الملف التجاري عدد 1356/1/2016.

وفي حكم أخر صادر عن المحكمة التجارية بمراكش قضت من خلاله بالتعويض للمدعية التي تضررت من استعمال شركة للاتصالات لبياناتها الشخصية بصورة مغلوطة حيث جاء في ادعاءات المدعية أن شركة الاتصالات قد أعطت لرجال الشرطة القضائية معلومات مغلوطة تفيد أنها قد اشترت منهم الخط الهاتفي الذي كان رجال الشرطة القضائية في إطار البحث عن صاحبه المتورط في قضية ما وهو

ما جعل العارضة تدخل في دوامة الاستدعاء والاستماع إليها من طرف الشرطة خاصة و أنه لم يسبق لها أن اشترت الخط الهاتفي من شركة الاتصالات وأن هذه الاخيرة استعملت المعلومات الشخصية والبيانات التي لديها بطريقة خاطئة وهو ما سبب ضررا لها فقضت المحكمة التجارية بما يلـي: (بتشطيب المدعى عليها من سجلاتها على بيان تملك المدعية لرقم النداء الهاتفي رقم .. وبأدائها لفائدتها تعويضا قدره 50.000 درهما) حكم عدد 537 بتاريخ 2021/2/18 ملف رقم 2020/8207/2074

حيث تعتبر هذه القضية صورة من صور المس بالمعطيات الشخصية فمن الرغم انه كان من الواجب على شركة الاتصالات تزويد عناصر الشرطة بالمعلومات الضرورية لبحثهم القضائي فإن ذلك رهين بصحة تلك المعلومات لا أن تكون معلومات مغلوطة لا تمس للواقع بصلة وعليه مجرد قيام شركة الاتصالات بتضمينها في سجلاتها للبيانات الشخصية للمدعية من غير إذن هذه الأخيرة يوجب مسؤوليتها بحسب قانون 08.09 المتعلق بالمس بالمعطيات الشخصية.

و كملاحظة مهمة في هذا السياق نلاحظ مع الأسف الشديد ان القضاء المغربي لازال وفيا في تطبيق المقتضيات القانونية للجرائم التقليدية على الجرائم الالكترونية ذلك انه من خلال استقرائي للحكم المشار اليه أعلاه لاحظنا ان تعليل المحكمة التجارية لهذة القضية جاء في سياق التعويض عن الضرر في اطار المسؤولية دون الإشارة لامن بعيد ولامن قريب الى ان وقائع النازلة موضوع الحكم تتعلق بالمس بالمعطيات الشخصية للمدعية.

كما جاء في قرار اخر لمحكمة النقض والذي يخص نفس السياق قضت بمقتضاه ما يلـي : **(أي شخص نشر صورتك بدون إذن منك من حقك اللجوء إلى القضاء من أجل المطالبة بالتعويض جبرا للضرر الناجم عن الفعل الضار، كما أن شخص نشر صورة الغير في مكان خاص دون موافقته يعد مرتكبا لجريمة يعاقب عليها بالحبس من سنة إلى ثلاث سنوات وغرامة من 2000 درهم إلى 20.000 درهم) قرار محكمة النقض عدد 3127.**

خــــاتمـــــــــــة

يظهر جليا من خلال دراستنا للامن السيراني في حماية المعطيات الشخصية على ضوء قانون 08.09 ان المشرع المرفيحقق قفزوة نوعية في مجال حماية المعطيات الخاصة للافراد خصوصا مع تنامي الاستعمال المكثف كما ونوعا للتكنولوجيا الحديثة .

والملاحظ أيضا ضعف الطابع الزجري بخصوص المقتضيات المتعلقة بحماية المعطيات الشخصية سواء على مستوى القانةن05.20 او على مستوى قانون 08.09 .

كما ان عدم وضوح الركن المعنوي للجرائم الماسة بالمعالجة يجعل هذه الاخيرة جرائم مادية محضة وهوما يمكن ايطرح عدة اشكالات تفعيل مقتضيات لبقانون08.09 امام القضاء. والملاحظ ايضا ان حماية المعطيات ذات الطابع الشخصي ليست مرادفا للحد من تداولها بل ترتكز على معالجة هذه المعطيات على نحو يضمن صون مصلحة المواطن.

ان حماية المعطيات الشخصية تستلزم ضمان موثوقية الاشخاص اللذين يعالجونها و تطوير النصوص القانونية الحالية و تحسيس المواطنين بنطاق وسيرورة الحماية و التوفر على رؤية استباقية تكفل استعاب التطور الرقمي الهائل.

الجلسة العلمية الخامسة

رئيس الجلسة

الدكتور طارق مصدق

أستاذ التعليم العالي، كلية العلوم القانونية والاقتصادية والسياسية – جامعة الحسن الأول سطات.

الأمن السيبراني وحرية التعبير عن الرأي في وسائل التواصل الاجتماعي وفق القانون العماني

الدكتور طلال بن سعيد بن ناصر المحاربي
مستشار قانوني (سلطنة عمان)

الملخص:

تتعرض مجتمعاتنا العربية لانتهاكات صارخة لقيمها الدينية ومبادئها وموروثاتها من العادات والتقاليد من قبل بعض مستخدمي وسائل التواصل الاجتماعي الذين يسعون إلى الوصول إلى الشهرة من خلال عرض وإنتاج مقاطع إما أن تكون غير أخلاقية أو أنها تعبر عن أفكار واعتقادات تمس بقيم المجتمع الدينية والأخلاقية وكذلك النظام العام، المشكلة أن غالبية أولئك الأفراد يتمسكون عند الحديث عن قيمة المحتوى والنتائج السلبية التي تترتب عليها بالحرية الشخصية والتعبير عن الرأي ، فكثير من رواد ومستخدمي وسائل التواصل الاجتماعي لا يستطيعون الفصل بين ما يعتبر في حدود التعبير عن الرأي وبين ما يعتبر مساساً بالنظام العام أو حقوق الاخرين.

صدر قانون الأمن السيبراني العماني بالمرسوم السلطاني رقم (2011/12) بمسمى قانون مكافحة جرائم تقنية المعلومات ليتحد مع باقي القوانين العقابية بالسلطنة مشكلاً هيكلة المعالجة القانونية لذلك النوع من الجرائم لذلك تأتي هذه الورقة البحثية لبيان الحدود الفاصلة بين ما يعتبر من قبيل الحرية الشخصية والتعبير عن الرأي، وبين ما يعد مساساً بالنظام العام للمجتمع العماني أو الأفراد في محاولة لإظهار تلك الحدود وإبرازها على النحو الذي يسهل معه التفريق بين الأمرين ، مع تسليط الضوء على أبرز تلك المسلكيات والمعالجة التشريعية العمانية لها، وسيتبع الباحث المنهج الوصفي التحليلي لنصوص مواد القانون حيث قسمت هذه الورقة إلى مبحثين الأول منهما خصص للحديث عن الحرية الشخصية والرأي والتعبير ، أما المبحث الثاني فقد خصص ليتناول جرائم التعبير عن الرأي في وسائل التواصل الاجتماعي ، وذلك في مطلبين الأول منهما سيسلط الضوء على جرائم الاعتداء على النظام العام ، أما المطلب الثاني فسيتناول جرائم الاعتداء على الأفراد، للوصول إلى الخاتمة.

Résumé:

Our Arab societies are exposed to flagrant violations of their religious values, principles and legacies of customs and traditions by some users of social media who seek to reach reputation by displaying and producing clips which is either immoral or express ideas and beliefs that affect the religious and moral values of the community as well as public order. The problem is that most of these individuals are cling of personal freedom and expression of opinion when talking about the value of content and the negative consequences that it entails, as many pioneers and users of social media cannot separate what is considered within the limits of expression of opinion and what is considered a violation of public order or the rights of others.

The Omani Cyber Security Law was issued by Royal Decree No. (12/2011) named cybercrime law to unite with the rest of the punitive laws in the Sultanate, forming the structure of the legal treatment for this type of crime. Therefore, this research paper comes to clarify the boundaries between what is considered as personal freedom and the expression of opinion, and what is considered a violation of the general order of the Omani society or individuals to show those limits and highlight them in a way that facilitates the differentiation between the two matters, highlighting the most prominent of these behaviors and the Omani legislative treatment of them. The paper is divided into two sections, the first of which is devoted to talking about personal freedom, opinion, and expression. In it, the researcher dealt with a statement of what freedom of opinion and expression is in a first demand, while the second requirement dealt with restrictions on freedom of opinion and expression. As for the second topic, it was devoted to dealing with the crimes of expressing opinion in social media, in two demands, the first of which will shed light on Crimes of assault on public order, and the second requirement will deal with crimes of assault on individuals, to reach the conclusion.

بسم الله الرحمن الرحيم

{مَنْ عَمِلَ صَالِحًا فَلِنَفْسِهِ وَمَنْ أَسَاء فَعَلَيْهَا ثُمَّ إِلَى رَبِّكُمْ تُرْجَعُونَ}

صدق الله العظيم. [الجاثية الآية 15].

مقدمة

شهد العالم تغيراً كبيراً في الأنماط الاجتماعية المكونة لعاداته وتقاليده بعد أن أتسع استخدام وسائل التواصل الاجتماعي وظهرت تطبيقات سهلة الاستخدام وواسعة الانتشار تهتم بتحقيق أكبر عدد ممكن من المشتركين بغض النظر عن قيمة المحتوى المنشور.

لذلك تتعرض مجتمعاتنا العربية لانتهاكات صارخة لقيمها الدينية ومبادئها وموروثاتها من العادات والتقاليد من قبل بعض مستخدمي وسائل التواصل الاجتماعي الذين يسعون إلى الوصول إلى الشهرة من خلال عرض وإنتاج مقاطع إما أن تكون غير أخلاقية أو أنها تعبر عن أفكار واعتقادات تمس بقيم المجتمع الدينية والأخلاقية وكذلك النظام العام، المشكلة أن غالبية أولئك الأفراد يتمسكون عند الحديث عن قيمة المحتوى والنتائج السلبية التي تترتب عليها بالحرية الشخصية والتعبير عن الرأي.

وهنا تكمن المشكلة فكثير من رواد ومستخدمي وسائل التواصل الاجتماعي يعجزون عن التميز بين حدي المعادلة، ولا يستطيعون الفصل بين ما يعتبر في حدود التعبير عن الرأي وبين ما يعتبر مساساً بالنظام العام، فيخرج بسلوكه ذاك عن حدود التعبير عن الرأي، ليقع في المحظور الذي يجعله عرضة للمساءلة القانونية.

ولخطورة جرائم تقنية المعلومات على الدولة والنظام العام من جهة وعلى الأفراد من جهة أخرى، فقد تصدى المشرع العماني لتلك الجرائم وأصدر قانون الأمن السيبراني بالمرسوم السلطاني رقم (2011/12) ويحمل مسمى قانون مكافحة جرائم تقنية المعلومات ليتحد مع باقي القوانين العقابية بالسلطنة مشكلاً هيكلة المعالجة القانونية لذلك النوع من الجرائم غالق الباب أمام كل من تسول له نفسه المساس بالنظام العام أو الاعتداء على الأفراد، وقد أعتمد المشرع العماني عند إصدار هذا القانون على اتفاقية بودابست وعلى التشريعات المحلية والإقليمية والدولية إدراكا منه بأهمية أن ينعم كل مواطن بحقه في الاستخدام الأمن لأجهزة الحاسب الألي وشبكة المعلومات الدولية .

لذلك تأتي هذه الورقة البحثية لبيان الحدود الفاصلة بين ما يعتبر من قبيل الحرية الشخصية والتعبير عن الرأي في وسائل التواصل الاجتماعي، وبين ما يعد مساساً بالنظام العام للمجتمع العماني في محاولة لإظهار تلك الحدود وإبرازها على النحو الذي يسهل معه التفريق بين الأمرين، مع تسليط الضوء على أبرز تلك المسلكيات والمعالجة التشريعية العمانية لها وذلك من خلال الآتي:

المبحث الأول : الحرية الشخصية والتعبير عن الرأي في وسائل التواصل الاجتماعي

المطلب الأول : ما هيه الحق في التعبير عن الرأي

المطلب الثاني : مظاهر حرية التعبير عن الرأي

المبحث الثاني : القيود على حرية التعبير عن الرأي في وسائل التواصل الاجتماعي

المطلب الأول : حماية النظام العام

المطلب الثاني : حماية حقوق وحريات الأفراد

الخاتمة

المبحث الأول: الحرية الشخصية والتعبير عن الرأي في وسائل التواصل الاجتماعي

حرصت أغلب التشريعات العربية على الاهتمام بالحرية الشخصية للإنسان تماشياً من مبادي الدين الإسلامي الحنيف، وما نصت عليه المعاهدات والمواثيق الدولية التي تعنى بحقوق الإنسان وحرياته، فقد احيطت تلك الحقوق بالضمانات القانونية التي تمنع المساس بها، ومن أبرز الحقوق الشخصية المقرر حمايتها الحق في التعبير عن الرأي ، أي حرية الأشخاص في تكوين أفكارهم والتعبير عنها بالطرق التي يرونها مناسبة وبالكيفية التي يختارونها ،

إلا أن ذلك لا يعني أنهم في ذلك أحرار بشكل مطلقة وبلا حدود وإلا تحولت إلى فوضى وحملت الكثير من الإساءة والاعتداء على الدولة وعلى حقوق الأخرين ، لذلك سنتناول في هذا المبحث مطلبين الأول منهما خصص لبيان ما هيه حرية الرأي والتعبير عنه ، أما الثاني فيتناول مظاهر حرية الرأي والتعبير .

المطلب الأول: ما هيه الحق في التعبير عن الرأي

الحق في حرية الرأي والتعبير في حقيقته هو شكلين متلازمين من أشكال الحرية الشخصية لا يمكن الفصل بينهما ولا يتصور قيام أحدهما دون قيام الأخر ، وهما حرية الرأي ، وحرية التعبير [259]، فلا يمكن أن يظهر الرأي إلى العالم الخارجي إلا عن طريق التعبير عنه ويستوي بعد ذلك الوسيلة المستخدمة لذلك التعبير ، سواءً كان بالقول أو بالكتابة أو بالإشارة الدالة عليه أو تناقلته وسائل تقنية المعلومات على شكل صور أو مقاطع مرئية أو غيره من أساليب التعبير ، وقد نص النظام الأساسي للدولة260 في المادة (35) منه على أن (حرية الرأي والتعبير عنه بالقول و الكتابة وسائر وسائل التعبير مكفولة في حدود القانون).

إلا أنه ورغم أن المشرع العماني نص صراحة على حرية الرأي والتعبير في النظام الأساسي للدولة إلا أنه لم يتطرق لأي تعريف عن ذلك الحق ، وقد أختلف الفقهاء في التعريف به فمنهم من قال بأنه(قدرة الإنسان على التعبير عن وجهة نظره بمختلف وسائل التعبير ، وأن يبينوا رأيهم في سياسة الحاكم التي تعود بالنفع عليهم)[261]، كما عرفه أخرون بأنه (حرية المواطن في أن يفكر ويعبر عن تفكيره بالأساليب المشروعة وحريته في نقد الأوضاع ، والأنظمة والاتجاهات والتصرفات دون أن يخشى على نفسه)[262]، وأجد أنه من الممكن تعريف حرية الرأي والتعبير بأنها قدرة الشخص على تكوين عقيدته في موضوع ما وإظهارها للغير بالطريقة التي يرى فاعليتها لإعلان رأيه،

ومن التعريف السابق يمكن القول أن هذه الحرية حقين الأول منهما حق الإنسان في حرية الرأي ويقصد بها مقدرة الشخص على تكوين رأيه بتفكيره الشخصي دون تدخل من أحد أو أن يكون مكره على اعتناق فكراً ما أو خائفاً من أحد ، وأن يتمتع ذلك الشخص بالحرية الكاملة في اختيار الوسيلة التي يراها مناسبة لإعلان رأيه وبالأسلوب الذي يناسبه[263]، وبالتالي لا يجوز محاسبة ذلك الشخص عما يتخذه من رأي أو الإضرار به فلكل شخص الحق في تبني ما يشاء من أفكار ، وقد أقرت غالبية المعاهدات والمواثيق الدولية ذلك فالمادة (19) من الإعلان العالمي لحقوق الإنسان نص على (حرية اعتناق رأي ما هي حرية مطلقة لا يجوز تقييدها

---

[259]. نزار أيوب ، حرية الرأي والتعبير في مناطق السلطة الوطنية الفلسطينية ، دراسة مقارنة في ضوء المواثيق الدولية لحقوق الإنسان والتشريعات الفلسطينية ، رام الله مؤسسة الحق ، 2001، ص2

[260] . النظام الأساسي للدولة الصادر بالمرسوم السلطاني (2021/6) ، الجريدة الرسمية رقم 1374

[261] . محمد الزجيلي ، حقوق الإنسان في الإسلام ، دار الكلم الطيب ، دمشق ، ط3، 2003، ص186

[262] . يوسف القرضاوي ، الحلول المستوردة وكيف جنت على أمتنا ، دار البعث للطباعة والنشر ، قسنطينة ، ط1، 1984، ص211-212

[263] خالد مصطفى فهمي ، حرية الرأي والتعبير ، دار الفكر الجامعي ، الإسكندرية ط1، 2009،ص19

بموجب القوانين أو من جانب أي سلطة أخرى) ، وتكوين الرأي وفق هذا المعني يشير إلى الحالة الذهنية للإنسان بحيث يفكر في شيء ما ويصل بشأنه إلى فكرة معينة ، وبالتالي فإن الرأي هو شي داخلي وخفي إلا إذا ظهر إلى العام الخارجي عن طريق التعبير عنه ، وبالتالي لا يمكن معاقبة الأشخاص عما يدور في أذهانهم من أفكار وقناعات حتى لو كانت تلك الفكرة تتعلق بارتكاب جريمة، فالجريمة تمر بعدة مراحل حتى تبرز إلى حيز الوجود ، المرحلة الأولى منها هي مرحلة التفكير والتصميم ،فالجريمة تبدأ بفكرة في ذهن الجاني ومن ثم التصميم والعزم على ارتكابها ، وهذه المرحلة لا يتخذ فيها ذلك التفكير أي مظهر خارجي وبالتالي لا يتدخل القانون للمعاقبة عنها ، وقد عبر المشرع العماني عن ذلك صراحة في المادة (29) من قانون الجزاء العماني (لا يعد شروعاً مجرد العزم على ارتكابها ...) إلا أن المشرع العماني تشدد في تجريم بعض الأفعال بالرغم من أن الجاني لم يدخل إلى مرحلة تنفيذ الجريمة وهي ما نصت عليه المادة (91) [264] من قانون الجزاء العماني إذ أعتبر القانون الاتفاق على ارتكاب جريمة من جرائم أمن الدولة جريمة قائمة حتى لو لم يبدأ الجاني في تنفيذ الفعل المكون للسلوك المادي للجريمة[265].

أما الحق الثاني فهو حرية التعبير ويقصد بها اختيار الشخص الوسيلة المناسبة للتعبير عن رأيه فهو حر في اختيار ما يراه مناسباً من طريقة أو وسيلة للتعبير عن أفكاره ومعتقداته وقناعاته، ولا يجوز أن يتدخل أي شخص لإرغام غيره على التعبير عن رأيه ، فإي تدخل في ذلك يعد إكراه ومساساً مباشرا بهذه الحرية ، وإذا كان الرأي هو أمر داخلي يدور في ذهن الإنسان فالتعبير هو المظهر الخارجي لذلك الرأي فعندما يعبر الشخص عن أرائه وأفكاره يكون بذلك قد تجاوز المرحلة السابقة على ارتكاب الجريمة وهي مرحلة التفكير والتصميم وبالتالي أي تعبير عن الرأي فيه مساس بالنظام العام يعد جريمة يعاقب عليها القانون .

المطلب الثاني : مظاهر حرية الرأي والتعبير

ممارسة الحق في الرأي والتعبير كغيرها من الحقوق الأخرى لها مظاهر معينة تظهر بها للعالم الخارجي، فهي ترتبط بحقوق أخرى كارتباط حق التعبير عن الرأي بحرية الأعلام بكافة أشكاله وأنواعه - ومنها الإعلام الالكتروني[266] - وحرية الحصول على المعلومات وحرية التجمع السلمي، بل أن ممارسة تلك الحقوق هو في

---

264 نصت المادة (91) على أنه (يعاقب بالسجن مدة لا تقل عن 3 سنوات ولا تزيد على 7 سنوات كل من : أشترك في اتفاق جرمي بغرض ارتكاب إحدى الجنايات المنصوص عليها في هذا الباب....)

265 د . عادل عبد إبراهيم العاني ، شرح قانون الجزاء القسم العام ، مكتبة الأجيال ،ط 1 ،2018 م ، ص134

266 أحمد نهاد أحمد الغول ، حرية الرأي والتعبير في المواثيق الدولية والتشريعات المحلية ، سلسلة تقارير قانونية (65).

حقيقته الجانب العملي لممارسة الافراد لحقهم في حرية الرأي والتعبير، وفيما يلي أبرز مظاهر حرية الرأي والتعبير:

الفرع الأول : حرية الطباعة والنشر

منذ القدم عرفت الكتابة كأهم وسائل التعبير عن الرأي ، فكانت من أوائل الوسائل التي استخدمها الإنسان لنقل ما يفكر فيه وما يدور في مخيلته من أفكار ومعلومات وكذلك العلوم والمعارف وكانت في بداية الأمر تمارس بشكل يدوي ، بعدها تطور الأمر عندما ظهرت الآت الطباعة اليدوية ومن ثم الحواسيب الحديثة ، والتي صاحبها ظهور المطبوعات الورقية بأنواعها – المجلات والصحف وغيرها - وأخيراً المطبوعات الالكترونية التي نالت اهتمام الجميع بعد أن أصبحت من أهم أشكال الطباعة والنشر ، فخلال السنتين الأخيرتين ومع انتشار جائحة كوفد 19 في العالم بدأت مؤسسات الصحافة والنشر التقليدية ابتكار وسائل حديثة لتحافظ على مكانتها من تلك الوسائل الصحف الالكترونية ، بل أن بعض الصحف التي كانت تصدر بشكلها الكلاسيكي المعروف - من الورق والحبر- لجأت إلى التحول الرقمي إثر هذه الجائحة، حرية الطباعة والنشر كأحد مظاهر التعبير عن الرأي نظمها قانون المطبوعات والنشر العماني[267] ،

فعندما يبدأ الإنسان في نقل أفكاره وآراءه لغيره فهو بذلك يمارس حقه في حرية التعبير المقررة بموجب المادة (35) من النظام الأساسي للدولة بالوسيلة التي رأى أنها الأنسب لتحقيق ذلك ، وهذه الوسيلة لا تقل خطورة عن خيرها من وسائل التعبير عن الرأي لذلك فهي تخضع لذات القيود المفروضة على حرية الرأي والتعبير[268] ، ففي الفصل الرابع من قانون المطبوعات والنشر تحت عنوان في المسائل المحظور نشرها حدد المشرع العماني القيود على الطباعة والنشر ، وهي المسائل التي من شأنها النيل من قائد البلاد وأفراد الأسرة المالكة الكريمة وكذلك النظام العام ، كما لا يجوز نشر كل ما من شأنه المساس بالأخلاق والأدب العامة والديانات السماوية ،كذلك لا يجوز نشر الأخبار أو الصور والتعليقات التي تتصل بأسرار الحية الخاصة أو العائلية للأفراد إلا إذا كان ذلك النشر تنفيذا لحكم قضائي أو قرار إداري تقتضيه المصلحة العامة وغيرها من القيود الأخرى المنصوص عليها في هذا القانون.

267 قانون المطبوعات والنشر رقم 84/49 ، الجريدة الرسمية رقم 289 ،الصادر في 1984/6/2م

268 . عبدالله خليل ، الحماية القانونية للصحفيين وأخلاقيات العمل الصحفي ، منشور على الصفحة الإلكترونية www.cdfj.org

الفرع الثاني: حرية النشر الالكتروني

مع التطور التكنولوجي الذي شهده العام إثر ظهور شبكة المعلومات الدولية بدأ النشر الإلكتروني يأخذ طريقة في الانتشار ليحتل مكانة متقدمة بين باقي وسائل النشر المعروفة ، فأصبحت الشبكة المعلوماتية وسيلة منافسة لوسائل التعبير التقليدية ، حيث أن الانترنت أتاح الفرصة للجميع أن يمارسوا حقهم في حرية والتعبير عن آراءهم ، فقد ورد في إعلان المبادئ الذي اعتمدته القمة العالمية لمجتمع المعلومات بجنيف في العام 2003 بأن حرية التعبير وحرية تدفق المعلومات والمعارف والأفكار والعلم ضرورية لمجتمع الإعلام وتعود بالنفع على التنمية، وتطبيقاً لذلك فقد تقدم مراسلون بلا حدود بمجموعة من التوصيات تتعلق بحرية التعبير على الشبكة المعلوماتية منها أن مستخدمو الانترنت وحدهم من يقررون المادة التي يمكنهم ويريدون الدخول عليها عبر الانترنت ومن غير المقبول أن تقوم الحكومات أو الشركات الخاصة، بالتنقية او التدقيق التلقائي على المواد الموجودة في الانترنت ، كذلك لا يجوز أن يتخذ قرار بإغلاق موقع الإلكتروني حتى وان كان ذلك الموقع غير قانوني من قبل الموقع المستضيف أو مقدم الخدمة التقنية، إلا من قبل القاضي [269]،وقد اصدرا لمحاكم العمانية خلال العام الجاري حكماً قضائياً يعد سابقة من نوعها قضاء بإغلاق حسابات الالكترونية لمراءتين قامتا بنشر مقاطع مرئية وصور تخل بالأدب العامة [270].

الفرع الثالث: حرية التجمع السلمي

يعد هذا المظهر من أقدم مظاهر التعبير المعروفة حيث وهو حق مكفول وفق القوانين كما أقرته المعاهدات والاتفاقيات الدولية ، حيث أكد عليه الإعلان العالمي لحقوق الانسان عام 1948، وكذلك المادة (21) من العهد الخاص بالحقوق المدنية والسياسية والتي نصت على أن (يكون الحق في التجمع السلمي معترفاً به ولا يجوز أن يوضع من القيود على ممارسة هذا الحق إلا التي تفرض طبقاً للقانون وتشكل تدابير ضرورية في مجتمع ديمقراطي ، لصيانة الأمن القومي أو السلامة أو النظام العام أو حماية الصحة العامة أو الأدب العامة أو حماية حقوق الأخرين وحرياتهم [271]، وبالرغم من أن التعبير عن الرأي مكفول وفق النظام الأساسي للدولة وبالتالي فأي وسيلة من تلك الوسائل تكون مشروعة شريطة أنها لا تمس بأمن المجتمع والنظام العام ـ لذلك فقد نص

---

269 أنظر الموقع الالكتروني WWW.radionongrata.og

270 انظر الموقع الالكتروني www.atheer.om

271 أحمد نهاد محمد الغول ، حرية الرأي والتعبير في المواثيق والتشريعات المحلية ، سلسلة تقارير قانونية (65) إنظر C:/Users/User/Downloads/legal65%20(2).pdf

المشرع على تجريم أي تجمع يهدف إلى الإخلال بالنظام العام وخلق فوضى وفقاً للمادة 137 من قانون الجزاء العماني .

المبحث الثاني: القيود التي ترد على حرية التعبير عن الرأي في وسائل التواصل الاجتماعي في القانون العماني

كفالة الحق في حرية الرأي والتعبير التي نص عليها النظام الأساسي للدولة كأحد المبادي الأساسية للحقوق والحريات ،أخذها البعض – للأسف الشديد - على إطلاقها فتجاوز بأفعاله ومسلكياته قصد الشارع ليتعدى على الغير بصور شتى ، فبوجود المحفزات التي توفرها وسائل التواصل الاجتماعي أصبح من الصعب - على البعض - الالتزام بالحدود التي رسمها القانون للتعبير عن آرائهم ، فوسائل التواصل الاجتماعي تشكل بيئة خصبة ومناسبة لانتهاك حرمة الحياة الشخصية للغير، وكذلك زعزعة الثقة بمؤسسات الدولة والحكومة ، والمساس بمكونات النظام العام من القيم والمبادئ الدينية والأخلاقية الراسخة ، فالمادة (35) من النظام الأساسي للدولة نصت على أن(حرية الرأي والتعبير عنه بالقول و الكتابة وسائر وسائل التعبير مكفولة في حدود القانون) ، وبالتالي فأن حرية الرأي مكفولة وفق هذه المادة إلا إذا خرج ذلك التعبير عن الرأي عما حدده القانون فإنه يعد جريمة تستوجب العقاب.

وكما بينا سابقا بأن وسائل التواصل الاجتماعي في وقتنا الحالي تمثل أهم وسائل التعبير عن الرأي، وبالتالي لا بد من ظهور بعض المسلكيات التي تخرج عن حدود التعبير المشروع عن الرأي لتمس بالنظام العام أو حقوق الأخرين وحرياتهم، وفيما يلي بيان للقيود التي تحكم حرية الرأي والتعبير في وسائل التواصل الاجتماعي وذلك وفق الآتي:

المطلب الأول: حماية النظام العام

يمثل النظام العام أحد أهم ركائز قيام الدول العربية لذلك نجد أن تلك الدول حريصة على فرض الحماية القانونية عليه ، وحظر المساس به أو الاعتداء عليه ، واعتبرت ذلك جريمة يعاقب عليها القانون ، ولما كانت وسائل التواصل الاجتماعي تمثل إحدى الوسائل التي يستخدمها الأشخاص في النيل من النظام العام والتعدي عليه وانتهاك مبادئه فقد حرص المشرع العماني على تجريم بعض المسلكيات التي قد تصدر من الأشخاص في وسائل التواصل الاجتماعي - على اعتبار أنها مظهر من مظاهر حرية التعبير عن الرأي المكفولة

قانوناً - بحق النظام العام ، وقبل الحديث عن تلك الجرائم لا بد من التطرق لتعريف النظام العام وبعدها سنتناول المسؤولية الجزائية التي تترتب على ذلك المساس وذلك وفق الآتي :

الفرع الأول: معنى النظام العام وعناصره

مصطلح النظام العام بشكله الذي هو عليه ليس مجرد فكرة ظهرت من العدم أو أوجدتها القوانين المعاصرة، وإنما تكونت هذه الفكرة إثر ما كان سائد في العصور الماضية من مظاهر القسوة والسيطرة التي يمارسها البعض ضد فئات محددة من العامة، فهي فكرة قامت إثر رغبة المجتمعات في التطور من خلال تصور ما هو مفيد لها ومرغوب فيها من مبادئ التنظيم الاجتماعي بما يحقق مصالح العامة، فكانت كل خطوة نحو ذلك تتبعها خطوة مماثلة في القانون الذي يحكم المجتمع بهدف تحقيق التوازن بين نصوص القانون وما يطمح إليه الأفراد في المجتمع لبناء كيانهم الاجتماعي [272].

وبالرغم من الحرص الكبير الذي توليه التشريعات العربية للنظام العام، إلا أنها لم تتعرض لهذه الفكرة بالتعريف وهذا أمر طبيعي، فالنظام العام فكرة مرنة تتغير وفقاً للزمان والمكان ووفقا لطبيعة الدولة وتشريعاتها الداخلية وما تحتويه تلك الدولة من العادات والتقاليد والأعراف، فالاختلاف في تلك الفكرة قائم على أساس تغير تلك الأسس من دولة الى أخرى، فما يعد مباحاً وجائز في بلد لا يعد كذلك في بلد أخر فهو مستهجن ومحظور.

المشرع العماني جرم أي اعتداء أو مساس بالنظام العام إلا أنه لم يتطرق -كذلك - لأي تعريف له، تاركاً المجال للمشتغلين في القانون والمهتمين به الأخذ بما توصل إليه فقها القانون من تعريف لهذه الفكرة ، حيث عرفة البعض قائلاً بأن قواعد النظام العام هي تلك القواعد الموضوعة لحماية المصالح حتى الفردية منها والتي تعتبر أساسية للمحافظة على سلام وازدهار المجتمع الاجتماعية موضوع الاهتمام [273]، كما عرفة أخرون بأنه مجموع المصالح الأساسية للجماعة أي مجموع الأسس والدعامات التي يقوم عليها بناء الجماعة وكيانها بحيث لا يتصور بقاء هذا الكيان سليماً دون استقراره عليه[274]، وقد عرف العهد الدولي الخاص بالحقوق المدنية والسياسية النظام العام على أنه مجموعة القواعد التي تؤمن السير العادي للمجتمع أو التي تشكل الأساس التي يقوم عليها المجتمع ، واحترام حقوق الانسان جزء من النظام العام، في حين أن الفقيه (شارل ديباش)

---

272 عبدالله محمد محمود ، المدخل إلى علم القانون أو النظرية العامة للقانون، ط7 ، مطبوعات جامعة دمشق ، 1996، ص51
273 عبد القادر عودة ، التشريع الجنائي الإسلامي مقارن بالقانون الوضعي ، مؤسسة الرسالة بيروت سوريا، ط3 ، 1994، ص152
274 زهدي يكن ، القانون الإداري منشورات المكتبة العصرية ، صيد بيروت ، د.ط.د.ت، ص77-78

عرف النظام العام على أنه (مفهوم متغير يلخص روح الحضارة وحقبة من الزمن وينطوي على مجموعة من المتطلبات التي تعد أساسية لحماية الحياة الاجتماعية [275])، وأجد أنه من الممكن تعريف النظام العام بإنه مجموعة من المبادئ الأساسية الملزمة التي تحكم سلوك الأفراد والدولة في أي مجتمع ، والنظام العام على النحو السابق بيانه يتكون من عدة عناصر وهي:

أولاً: الأمن العام.

يعد الأمن العام العنصر الأول من عناصر النظام العام ويقصد به حماية الأرواح والأموال من كل خطر يهددها سواءً كان مصدر هذا الخطر يرجع إلى فعل الإنسان أو فعل الطبيعة أي تأمين الأفراد في مالهم وأنفسهم [276]، كما كل ما يطمأن الإنسان على مالة ونفسه وذلك بمنع وقوع الحوادث أو احتمال وقوعها والتي من شأنها إلحاق الأضرار بالأشخاص والأموال وعليه فأن مفهوم الأمن العام من جهة الدولة يعني المحافظة على السلامة العامة بالعمل على درء ومنع المخاطر التي تهدد الأفراد بطريقة وقائية قبل وقوعها وبالتالي لسلطات الأمن العام اتخاذ كافة التدابير والإجراءات من أجل منع ارتكاب أي جريمة أو منع وقوع أي خطر يؤثر على أمن أفراد المجتمع[277]، وبالتالي فإن الاستخدام السيء لوسائل التواصل الاجتماعي بنشر ما يؤثر على الأمن العام يعد مساساً بالنظام العام ولو كان تعبيراً عن الرأي .

ثانياً: الصحة العامة.

وتعني الأوضاع الصحية للشعب بأكمله أو الجماعة ككل وانعدام الأمراض والأوبئة وأسباب الوفاة أي سلامة الأوضاع الصحية للمجتمع [278]، وبالتالي فهي كما عرفت منظمة الصحة العالمية الصحة العامة على أنها حالة اكتمال السلامة جسدياً وعقلياً واجتماعياً لا مجرد انعدام المرض والعجز[279]، وأكبر مثال لمفهوم الصحة العامة ما نراه من إجراءات وتدابير وما يصدر من قرارات وتوجيهات وما يرسم من سياسات لمواجهة الانتشار الواسع للوباء Covid 19 بهدف تحقيق الصحة العامة للمجتمع ويأتي قانون مكافحة الأمراض المعدية الصادر

---

275 د . سليمان الطماوي ، الوجيز في القانون الإداري ، دار الشروق ، القاهرة ، 1967، ص 491

276 د. أحمد عبدالرحمن شرف الدين – مبادي القانون الإداري – دار الفكر المعاصر – 2002- ص108

277 فيصل نسيغة ، النظام العام ، بحث منشور في مجلة المنتدى القانوني العدد الخامس، جامعة محمد خيضر بسكرة، ص173
http://archives.univ-biskra.dz

278 محمد الغمري ص9

279 تعريف منظمة الصحة العالمية

HTTP://WWW.PHRMOVMENT.ORG/PDF/CHARTER

بالمرسوم السلطاني رقم 92/73 كأحد القوانين التي تنظم تدابير الصحة العامة في السلطنة ، لذلك فقيام أي شخص بالتعبير عن رأيه في وسائل التواصل الاجتماعي بما يخالف تدابير الصحة العامة أو انتقادها على النحو الذي يشكك في فاعليتها في المحافظة على الصحة العامة أو تحسينها ، يعد مخالفاً للنظام العام ومعتدياً عليه، وهناك ارتباط وثيق بين الصحة العامة والأمن العام ، لأن المحافظة على الصحة العامة من شأنه زيادة الإنتاج الذي يترتب عليه زيادة الدخل وبالتالي نقصان في نسبة ارتكاب الجرائم[280] .

ثالثاً: السكينة العامة.

هي العنصر الثالث من عناصر النظام العام ، ويقصد بها اتخاذ الإجراءات الكفيلة لضمان الهدوء العام وحظر كافة مظاهر الإزعاج والمضايقات شريطة أن لا تتجاوز تلك المضايقات الحد المألوف الذي تفرضه الحياة داخل المجتمع ويشترط أن تصل إلى حد من الجسامة يستدعي تدخل السلطات المختصة [281]، كمن يستخدم مكبرات الصوت في حفلات الزفاف وفي ساعات متأخرة من الليل للدرجة التي تزعج الأخرين من سكان الحي ، وكمن يستخدم بوق المركبة بشكل مزعج أو كلعب كرة القدم في المناطق السكنية وفي غير الأماكن المخصصة ، ولأهمية السكينة العامة ذهب بعض الفقهاء إلى أنه نتيجة للتقدم التكنولوجي أصبحت محاربة الضوضاء تتجاوز مفهوم السكينة العامة وأصبحن تتلاقى مع فكرة الصحة العامة والأمن العام[282]، ومن تدابير السكينة العامة قيام الحكومة بتخصيص أماكن محددة للمناطق الصناعية تكون مستقلة وبعيدة عن مناطق سكنى الأفراد وذلك لضمان الهدوء والسكينة في المناطق السكنية.

الفرع الثاني: المسؤولية الجزائية الناتجة عن المساس بالنظام العام

تناول القانون العماني المسؤولية الجزائية الناتجة عن استخدام وسائل تقنية المعلومات أو شبكة المعلومات الدولية في التعبير عن الرأي بشكل يمس بالنظام العام في المادة 19 من قانون مكافحة جرائم تقنية المعلومات ، حيث أن هذه المادة بينت بدقة حدود حرية التعبير عن الرأي في وسائل التواصل الاجتماعي إذ نصت على أن (يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال ولا تزيد على ثلاثة آلاف ريال عماني أو بإحدى هاتين العقوبتين كل من استخدم الشبكة المعلوماتية أو وسائل تقنية

---

280 د محمود أبو السعود حبيب ، القانون الإداري ، دار الثقافة الجامعية ، 1999 ، ص188

281 د.داود الباز ، حماية السكينة العامة معالجة لمشكلة العصر في فرنسا ومصر الضوضاء – دار الفكر العربي -2004 - ، ص128 -135

282 د. محمد احمد فتح الباب السيد ، سلطات الضبط الإداري في مجال ممارسة حرية الاجتماعات العامة – رسالة دكتوراة جامعة عين شمس ، 1993 ، ص96

المعلومات في إنتاج أو نشر وأو توزيع أو شراء أو حيازة كل ما من شأنه أو ينطوي على المساس بالقيم الدينية أو النظام العام)[283]. ولقيام المسؤولية الجنائية وفقاً لهذه المادة لا بد من توافر شروط معينة وهي :

أولاً: استخدام الشبكة المعلوماتية أو وسائل تقنية المعلومات في ارتكاب الفعل .

نظراً إلى أن هذه الجريمة من جرائم المحتوى الالكتروني، التي نص عليها المشرع في الفصل الخامس من قانون الأمن السيبراني العماني المسمى بقانون مكافحة جرائم تقنية المعلومات فلا بد لقيامها أن يكون باستخدام الشبكة المعلوماتية أو وسائل تقنية المعلومات وقد عرف قانون مكافحة جرائم تقنية المعلومات المصطلحين في الفصل الأول منه ،حيث عرف الشبكة المعلوماتية على أنها ارتباط بين أكثر من وسيلة لتقنية المعلومات للحصوص على البيانات والمعلومات الالكترونية وتبادلها ، في حين عرف وسائل تقنية المعلومات على أنها جهاز الكتروني يستخدم لمعالجة البيانات والمعلومات الالكترونية أو تخزينها أو إرسالها أو استقبالها كأجهزة الحاسب الألي وأجهزة الاتصال، وبالتالي لا يتصور قيام هذه الجريمة بغير ذلك فقيام الشخص بنشر أوراق ومنشورات مكتوبة تنطوي على مساس بالنظام العام لا يعد من الجرائم الإلكترونية التي ينطبق عليها هذا القانون[284] وإن كان يمثل جريمة عادية وفق قانون الجزاء العماني، بعد ذلك يستوي في قيام المسؤولية الجزائية وفق هذا القانون كافة البرامج والتطبيقات والمواقع والمنتديات وغيرها من الوسائل التي تستخدم شبكة المعلومات الدولية أو وسائل تقنية المعلومات .

ثانياً: أن يتخذ الفعل المادي المكون للسلوك الجرمي أحد الصور المبينة في المادة .

لا بد لقيام أي جريمة من توافر الفعل المادي من بين العناصر الأساسية التي يتألف منها الركن المادي لتلك الجريمة ، ويتعذر الحكم بأية عقوبة إذا انتفاء ذلك الفعل، ويعرف الفعل المادي بأنه المظهر الخارجي للإرادة الاثمة ويتحقق بتصرف معين[285]، وقد بينت المادة (19) من القانون مكافحة جرائم تقنية المعلومات حصراً صور الفعل المادي المجرم وهو إنتاج، أو نشر أو توزيع أو شراء أو حيازة، وبالتالي فإن السلوك المكون لهذه الجريمة لا يخرج عن تلك الأفعال ، وكما هو واضح أنه يتخذ صورة العمل الإيجابي الذي يعبر عن حركة عضوية إرادية أي أن لذلك الفعل كيان مادي محسوس يتمثل بما يصدر من مرتكب الفعل من حركات لأعضاء

---

283 قانون مكافحة جرائم تقنية المعلومات ، صدر بالمرسوم السلطاني رقم 2011/12م، المنشور في الجريدة الرسمية رقم (929)، الصادرة بتاريخ 15/2/ 2011.

284 عرفت الفقرة ج من المادة 1 من الفصل الأول من قانون مكافحة جرائم تقنية المعلومات جريمة تقنية المعلومات بأنها الجرائم المنصوص عليها في هذا القانون .

285 د . عادل عبد إبراهيم العاني ، شرح قانون الجزاء العماني القسم العام ، مكتبة الأجيال ، ط1، 2018م ،ص 115

جسمه من أجل تحقيق أثر مادي معين [286]، ولا يتصور أن يقوم هذا الفعل بحركة عضوية فقط – أيا كان هذا الفعل – بل أنه يقوم بحركة عضوية ناتجة عن إرادة صادرة عن الجاني [287] ، فلا تقوم هذ الجريمة بالسلوك السلبي أي الامتناع عن القيام بعمل يفرضه القانون، فقيام شخص باستخدام وسائل التواصل الاجتماعي في نشر أخبار وإشاعات تتعلق بالنظام العام يعد جريمة وفق تلك المادة ، ومن الملاحظ في هذه المادة أن المشرع كان دقيقاً في تحديد الفعل المادي المكون للسلوك الجرمي من خلال بيان صور ذلك السلوك ، وفي هذه الحالة لا يتصور قيام الجريمة المنصوص عليها في هذه الجريمة دون توافر إحدى تلك الصور، والملاحظ أن تلك الأفعال من حيث الأصل هي أفعال مباحة غير مجرمة ، ولا يعني توافرها قيام الجريمة الإلكترونية، إلا إذا شكلت تلك الأفعال اعتداءً على النظام العام أو مبادي الدين الحنيف أو مست بحقوق الأخرين وحرياتهم.

ثالثاً: أن يكون فعل الجاني من شأنه أو ينطوي على مساس بالقيم الدينية أو النظام العام.

لا يكفي لقيام أحد الجرائم المنصوص عليها في هذه المادة استخدام الجاني لوسائل تقنية المعلومات أو الشبكة المعلوماتية كما لا يكفي أن يقوم بأحد صور الفعل المادي المكون للسلوك الجرمي ، وإنما يجب أن يكون المحتوى الذي قام بإنتاجه أو نشره أو توزيعة أو شراءه أو حيازته من شأنه أو ينطوي على مساس بالقيم الدينية أو النظام العام ، والقيم الدينية هي تلك القيم التي مصدرها الدين الإسلامي الحنيف كالعدل والمساواة بين أفراد المجتمع وحقوق الإنسان وكرامته ، والتسامح بين أفراد المجتمع بعضهم البعض ومع الأخرين ، والسلم [288]، أما النظام العام فقد تم بيان ما هيته ومكوناته فيما سبق، وبتالي يندرج تحت هذا التجريم كل فعل من الأفعال المنصوص عليها في هذه المادة إن مس بالنظام العام ومكوناته أو بالقيم الدينية، وبالتالي تدخل في دائرة هذا التجريم العديد من الجرائم المنصوص عليها في باقي القوانين العقابية مثال ذلك أن يقوم أحد الأفراد بالتعبير عن استياءه من السياسة الداخلية أو الخارجية للبلد ونشرها عبر مختلف وسائل التواصل الاجتماعي ، فإن ذلك يدخله في دائرة جرائم أمن الدولة التي نص عليها المشرع العماني في الباب الأول تحت عنوان الجرائم الماسة بأمن الدولة في المواد من 87 – 145 من قانون الجزاء العماني وكذلك مخالفة قانون مكافحة جرائم تقنية المعلومات .

---

286 د . عادل عبد إبراهيم العاني ، المرجع السابق ، ص 116

287 د. مجمود نجيب حسني ، شرح قانون العقوبات القسم العام ،ط6، دار النهضة العربية 1982،5،1989،ص 270-272

288 فاطمة طاهري ، القيم الدينية للثورة التحريرية الجزائرية كفكر وممارسة ، ملخص رسالة دكتوراه منشور على الموقع الالكتروني https://www.pnst.cerist.dz

عليه لا يجوز بأي شكل من الأشكال استخدام وسائل التواصل الاجتماعي في المساس بالنظام العام ويجرم أي فعل يقوم به الشخص يتضمن تعبيرا عن الرأي بشكل يقلل من شأن مؤسسات الدولة أو يضعف من مكانتها أو يحقر أداءها، كما يجرم أيضاً أي رأي عبر عنه صاحبة بأحد وسائل التواصل الاجتماعي وانطواء على مساس بالصحة العامة للمجتمع كمن يعبر عن رأيه في فاعلية لقاح ما أو دواء ما أو الطعن في مؤسسة صحية أو نشر شائعات تتعلق بانتشار وباء جديد في بلد ما، وكذلك من قام بالتشكيك في القرارات والإجراءات والقوانين التي تنظم تدابير الصحة العامة في المجتمع.

المطلب الثاني : حماية حقوق وحريات الأخرين

لم يقصر المشرع العماني عنايته على حق الرأي والتعبير - فقط - بل كان حريصاً على أن يقرر الحماية والاحترام لكافة الحقوق اللصيقة بالإنسان فجرم المساس بها أو الاعتداء عليها بأي شكل من الأشكال، حيث جعلها حقوق دستورية مقررة وفق الباب الثالث من النظام الأساسي للدولة تحت عنوان الحقوق والواجبات العامة، وبالتالي فإن أي مساس بتلك الحقوق يعد جريمة يعاقب عليها القانون، أياً ما كان شكل هذا المساس وأياً ما كانت الوسيلة المستخدمة ، فكما أن الجريمة من الممكن أن ترتكب بالطريق العادي الكلاسيكي أي الاعتداء المباشر على الحق محل الحماية القانونية ، كضرب المجني عليه أو شتمه أو قذفة أو انتهاك حرمة حياته الخاصة بشكل مباشر ووجه لوجه ، من الممكن كذلك ارتكابها بشكل الكتروني عبر وسائل تقنية المعلومات وعبر الشبكة المعلوماتية ، كمن يشتم غيره في أحد برامج التواصل الاجتماعي أو يلتقط الصور له أو أفراد أسرته في وضع لا يقبل به ودون علمه وبدون موافقته ، هنا كان القانون العماني حريصاً على أن تقوم المسؤولية الجزائية بحق من يستخدم وسائل تقنية المعلومات في المساس بتلك الحقوق الدستورية، وقبل الخوض في المسؤولية الجزائية الناتجة عن التعبير عن الرأي عبر وسائل التواصل الاجتماعي بشكل يسيء إلى الأخرين ويمس بحقوقهم وحرياتهم نتناول بإيجاز بعض تلك الحقوق والحريات الشخصية التي قررها المشرع العماني في النظام الأساسي للدولة وذلك وفق الآتي :

الفرع الأول: حقوق الأفراد في المجتمع

نص النظام الأساسي للدولة على جملة من الحقوق والحريات للأفراد والتي لا يجوز المساس بها أو الاعتداء عليها إلا وفق ما يحدده القانون ، وبالتالي المساس المسموح به في مجال الحقوق والحريات هو المساس الذي ينظمه القانون أو يسمح به، وتلك الحقوق والحريات المكفولة بالنظام الأساسي للدولة هي حقوق

وحريات مهمة ليعيش الأفراد في المجتمع دون خوف أمنين مطمئنين على أنفسهم، ونظراً إلى تعدد تلك الحقوق وتنوعها فلا يستوعب موضوعنا هذا تناولها بشكل تفصيلي لذلك سنكتفي بالتطرق إلى بعض تلك الحقوق بشيء من الإيجاز وذلك وفق الآتي:

أولاً: حق الإنسان في الحياة والكرامة.

تناول النظام الأساسي للدولة حق الإنسان في الحياة في المادة (18) منه حيث نص على أن (الحياة والكرامة حق لكل إنسان وتلتزم الدولة باحترامها وحمايتها وفقاً للقانون) كما أن هذا الحق له أسس دينية ، حيث أعتبر الإسلام الحق في الحياة مكفول للجميع فلا يجوز الاعتداء على حياة الأخرين، فحرم قتل الغير وكذلك قتل النفس قال تعالى (وَلا تَقْتُلُوا النَّفْسَ الَّتِي حَرَّمَ اللَّهُ إِلَّا بِالْحَقِّ)[289]وقال تعالى ((.. وَلَا تَقْتُلُوا أَنْفُسَكُمْ إِنَّ اللَّهَ كَانَ بِكُمْ رَحِيمًا)[290]،

ولضمان حماية أنفس الأخرين فقد عاقب الإسلام كل من يعتدى على حياة الغير بالقصاص وهو أشد أنواع العقوبات في الإسلام، قال تعالى(كُتِبَ عَلَيْكُمُ الْقِصَاصُ فِي الْقَتْلَى)[291]، وقال (وَلَكُمْ فِي الْقِصَاصِ حَيَاةٌ يَا أُولِي الأَلْبَابِ)[292] ،

كما أن هذا الحق حظى باهتمام المواثيق والاتفاقيات الدولة التي تعنى بحقوق الإنسان فقد نصت المادة الثالثة من الإعلان العالمي لحقوق الإنسان على (لكل فرد الحق في الحياة والحرية وسلامة شخصه، كما نصت المادة 1/6 من الاتفاق الدولي للحقوق المدنية والسياسية على أن(كل كائن بشري يتمتع بحق الحياة المتأصل فيه ، وهذا الحق يحميه القانون، ولا يحرم أحدا من هذا الحق بطريقة تعسفية)[293]،

أما المشرع العماني فقد كان حريصاً على حماية حق الإنسان في الحياة فبعد أن نص على هذا الحق على اعتباره أحد الحقوق الدستورية جرم أي اعتداء على حياة الأخرين ، حيث نصت المادة (301) من قانون الجزاء العماني على أن (يعاقب بالسجن المطلق كل من قتل إنسان عمداً) كما تضمنت المواد اللاحقة عليه

---

289 سورة الإسراء الآية 33

290 سورة النساء الآية 29

291 سورة البقرة الآية 178

292 سورة البقرة الآية 179

293 د . غازي حسن صباريني ،الوجيز في حقوق الانسان وحرياته الأساسية ، دار الثقافة للنشر والتوزيع ، الأردن ، ط4، 2015، ص117

أشكال ذلك الاعتداء على حياة الأخرين في صوره المشددة وكذلك المخففة ، وطبعاً لا يكفي أن يتمتع الإنسان بحقه في الحياة بل يجب أن تكون تلك الحياة كريمة وفق ما يقرره القانون من حقوق وواجبات.

ثانياً: حق الأفراد في سلامة جسدهم.

يقصد بحق الأفراد في سلامة جسدهم أي حقهم في الحماية القانونية التي تحول دون الاعتداء عليهم من قبل الأخرين ، فأي إيذاء يقع بحق جسم الإنسان يعد جريمة وفق النظام الأساسي للدولة وما قرره قانون الجزاء العماني من عقوبات لجرائم الإيذاء، ويقصد بجرائم الإيذاء ، الاعتداء غير المشروع على حق المجني عليه في سلامة جسمه أو الوظائف الطبيعية لأعضائه، وهذه المصلحة يحميها القانون وتشترك هذه الجرائم في محل الاعتداء مع جرائم القتل فمحلها الإنسان الحي ، وتختلف عنها أن الأولى يهدف إلى إزهاق روح الإنسان في حين أن هذه الجرائم تهدف إلى إصابة الإنسان بضرر جسدي أو صحي[294]،

وقد حرص المشرع العماني على تقرير الحماية الجزائية لهذا الحق فبعد أن نص على هذا الحق في النظام الأساسي للدولة كأحد الحقوق الدستورية قرر إنزال العقوبة على كل من يعتدي على حق الأفراد في سلامة جسمهم حيث تناول في المواد (307 وحتى 309) من قانون الجزاء صور الاعتداء الذي يقع على جسم الإنسان وتفاوت العقوبة نزولا وارتفاعا وفق ما يرتبه ذلك الاعتداء من ضرر في جسم المجني عليه.

ثالثاً: حماية حق الأفراد في حرمة المساكن

أراد المشرع العماني أن يحافظ على مكانة مسكن الأفراد على اعتبار أنه المكان الذي يعد مقراً لسكينة الافراد ومخزن أسرارهم ومستودع الحياة الخاصة التي لا يجب المساس بها أو الاعتداء عليها ، فنص في النظام الأساسي للدولة في المادة (33) على (للمساكن حرمه فلا يجوز دخولها بغير إذن أهلها إلا في الأحوال التي بينها القانون وبالكيفية المنصوص عليها في القانون)

وبالتالي فإن لمسكن الأفراد حرمة يجب أن تحترم وأن تحمى مخافة أن تنتهك من قبل البعض ، ولحماية هذا الحق جرم قانون الجزاء العماني أي اعتداء على ذلك الحق بالدخول بغير إذن من له الحق في أن يأذن بذلك وفي غير الأحوال التي يجيز فيها القانون ذلك، ففي المادة 371 من قانون الجزاء العماني (يعاقب بالسجن مدة لا تقل عن 3 أشهر ولا تزيد عن سنتين كل من دخل مكاناً مسكناً و معدا للسكنى أو أحد ملحقاته بغير

294 د عادل عبد إبراهيم العاني، شرح قانون الجزاء العماني القسم الخاص الجرائم الواقعة على الأشخاص والأموال ،شركة مطابع الباطنة ومكتباتها للطباعة التكنولوجية الحديثة ، ط1 ، 2021 ، ص125

رضى من له الحق في منعه من الدخول ، وفي غير الأحوال التي يجيزها القانون ، وتكون العقوبة السجن مدة لا تقل عن سنة ولا تزيد على 3 سنوات وإذا وقع الفعل ليلاً أو بواسطة الكسر أو التسور أو التسلق أو كان الجاني حاملاً سلاحاً أو ارتكب من شخصين فأكثر ، أو من شخص انتحل صفة عامة ، أو ادعى قيامه بوظيفة عامة).

رابعاً: حرمة الحياة الخاصة للأفراد.

نصت المادة (12) من الإعلان العالمي لحقوق الإنسان على أنه (لا يجوز أن يتعرض أحد لتدخل تعسفي في حياته الخاصة أو مسكنة أو مراسلاته أو لحملات على شرفه وسمعته ، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات)[295]، كما أن حرمة الحياة الخاصة تمتد لمسكنة فيمنع دخولها دون إذن منه إلا وفق ما يقرره القانون من حالات وإجراءات[296]، كذلك الحال بالنسبة للمراسلات فتعد من الحياة الخاصة التي لا يجوز الاطلاع عليها أو نشرها أو اختراقها إن كانت الكترونية على النحو والذي يمس من حرمتها ، وقد أكدت المادة (36) من النظام الأساسي للدولة بأن (للحياة الخاصة حرمة ، وهي مصونة لا تمس وللمراسلات الالكترونية بكافة أنواعها والمراسلات الهاتفية والبرقية والبريدية من وسائل الاتصال حرمة وسريتها مكفولة فلا يجوز مراقبتها أو تفتيشها أو الاطلاع عليها أو افشاء سريتها أو تأخيرها أو مصادرتها إلا في الأحوال التي يبينها القانون ووفق الإجراءات المحددة فيه)،

وللحياة الخاصة وفق هذه المادة مفهوم معين مضمونه حرية الإنسان في اختيار أسلوب حياته بعيداً عن التدخل وبدون أن يطلع على تفاصيل حياته أي شخص ودون أن ينقل شي منها إلى خارج محيط من يشاركه تلك الحياة الخاصة ، ويدخل تحت مضمون الحياة الخاصة كل ما يتعلق بالشخص من أمور تتعلق بحياته الأسرية أو العائلية أو المهنية أو ما يخص أسراره التي لا يحق للأخرين الاطلاع عليها كعلاقاته العاطفية أو أوضاعه الصحية أو وغيرها ، وأي اعتدا على حرمة تلك الحياة يشكل جريمة يعاقب عليها القانون .

---

295 أنظر المواد (17) من الدولي للحقوق المدنية والسياسية ، والمادة (8) من الاتفاقية الأوربية لحقوق الإنسان والمادة (11) من الاتفاقية الامريكية لحقوق الأنسان

296 د. عثمان عبد الملك صالح ، حقوق الأمن الفردي في الإسلام ، دراسة مقارنة بالقانون الوضعي ، مجلة الحقوق .ع3/س7، 1983 ، ص26

الفرع الثاني: المسؤولية الجزائية الناتجة عن الاعتداء على حرمة الحياة الخاصة باستخدام وسائل التواصل الاجتماعي

تناول المشرع العماني المسؤولية الجزائية الناتجة عن استخدام وسائل تقنية المعلومات أو شبكة المعلومات الدولية في التعبير عن الرأي بشكل يمس بحرمة الحياة الخاصة في المادة 16 من قانون مكافحة جرائم تقنية المعلومات والتي نصت على أن (يعاقب بالسجن مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن ألف ريال ولا تزيد على خمسة ألاف ريال عماني أو بإحدى هاتين العقوبتين كل من استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات كالهواتف النقالة المزودة بألة تصوير في الاعتداء على حرمة الحياة الخاصة أو العائلية للأفراد وذلك بالتقاط صور أو نشر أخبار أو تسجيلات صوتية أو مرئية تتصل بها ولو كانت صحيحة أو في التعدي على الغير بالسب أو القذف)، من ذلك يمكن القول أن هذه المادة ترتب المسؤولية الجزائية تجاه من يستخدم وسائل تقنية المعلومات أو شبكة المعلومات الدولية في التعبير عن الرأي بشكل يمس بحرمة الحياة الخاصة للأفراد، وهذه المساس لا يخرج عن الصورتين الآتيتين:

أولاً: التشهير وإساءة سمعة الغير

التشهير وإساءة السمعة تعني إشاعة السوء عن إنسان بين الناس[297]، أما الإساءة للسمعة فيقصد بها قيام شخص بنشر معلومات غير صحيحه تسيء لشرف شخص أخر أو أسرته[298]، وهناك فرق بين التشهير ولإساءة للسمعة فالأولى لا تكون إلا بإظهاره للناس وإعلانه لهم بأي وسيلة ، وقد يكون هذه التشهير يمس العرض والشرف والنسب وغيرها من الأمور الخاصة بالشخص ، أما الإساءة للسمعة فهي تمس بشكل أساسي بالعرض والشرف[299]، وقد بين المشرع العماني في المادة 16 من قانون مكافحة جرائم تقنية المعلومات صور التعدي المؤثم على حرمة الحياة الخاصة للأفراد، وهي :

☐. التقاط الصور باستخدام الهواتف النقالة التي تحتوي على كاميرات منتهكاً حرمة الحياة الخاصة للأفراد كمن يلتقط صور أفراد عائلة أحد الأشخاص أو منزله أو مركبته الشخصية أو أجزاء مخفية من

---

297 المقدم .د.مسفر بن حسن مسفر القحطاني ، الحماية المدنية للمعلومات الحاسوبية الشخصية(التعويض) في الفقه الإسلامي وأنظمة المملكة العربية السعودية ، مركز البحوث والدراسات بكلية الملك فهد الأمنية ،2005، ص74

298 محمود نجيب حسني ، شرح قانون العقوبات ، القسم الخاص ـ جرائم الاعتداء على الأشخاص ، 1981م ص660 ، وفوزية عبد الستار ، شرح قانون العقوبات القسم الخاص ، دار النهضة العربية ، القاهرة ،1982م ، ص 567.

299 عبد الواحد كرم ، معجم مصطلحات الشريعة والقانون ، دار المناهج ، الأردن ،ط2، 1998م، ص231.

منزله، ومن الملاحظ أن المشرع في هذه الصورة أعتبر مجرد التصوير اعتداء يستوجب العقاب حتى لو لم يتبعه أي نشر.

- أما الصورة الثانية من صور هذا الاعتداء فتتمثل في نشر الأخبار المتعلقة بحرمة الحياة الخاصة، كمن يتحدث عن خلافات عائلية واقعة في إحدى الأسر وينشر تفاصيلها، أو أنه يبدي رأيه فيها ، ولا يكفي أن يقوم الشخص بكتابة خبر ما وحفظه فلا بد أن يقوم بنشره لتقوم هذه الجريمة ، فالتعبير عن الرأي في هذه الصورة من صور المسؤولية الجزائية هي أساس التجريم فلا تقوم الجريمة إلا إذا عبر عنها بالنشر في إحدى وسائل تقنية المعلومات أو شبكة المعلومات الدولية.

- أما الصورة الثالثة من صور الاعتداء فهي التسجيل الصوتي أو المرئي، فالقانون لا يجيز تسجيل المحادثات أو ما يدور بين الأشخاص من حديث سواءً أكان ذلك الحديث عبر وسائل الاتصال أو كان بشكل مباشر أثناء تواجد الشخص في نفس المكان فقد نصت المادة (90) من قانون الإجراءات الجزائية على أنه (لا يجوز ضبط المراسلات والبرقيات أو الاطلاع عليها أو ضبط الجرائد والمطبوعات والطرود أو تسجيل الأحاديث التي نجرى في مكان خاص أو مراقبة الهاتف أو تسجيل المكالمات بغير إذن من الادعاء العام) حتى لو كان ذلك بغرض كشف جريمة ما، بل رتب المشرع جزاءً إجرائياً على مخالفة ذلك وهو البطلان في الدليل المتحصل من ذلك حيث نصت المادة (208) من قانون الإجراءات الجزائية على أنه(يترتب البطلان على عدم مراعات أحكام القانون المتعلقة بأي إجراء جوهري)، ومن الملاحظ على المادة (16) من قانون مكافحة جرائم تقنية المعلومات اشترطت لقيام المسؤولية الجزائية في هذه الصورة من صور الاعتداء على حرمة الحياة الخاصة قيام الجاني بنشر المقطع الصوتي أو المرئي الذي قام بتصويرة ، فلا تقوم الجريمة إلا بنشر تلك المقاطع ، أما إن ثبت عدم نشرها فلا مجال لمعاقبة الجاني عن تلك الجريمة .

ثانياً: التعدي على الغير بالسب أو القذف

يمثل السب والقذف أحد صور الاعتداء على حرمة الحياة الخاصة للآخرين التي نصت عليها المادة (16) من قانون مكافحة جرائم تقنية المعلومات ، والسب والقذف كلا منهما يمثل جريمة مستقله ، فالقذف هو إسناد واقعة محددة تستوجب عقاب من تنسب إليه أو احتقاره إسناداً علنياً عمداً[300]، على ذلك فإن القذف يقوم على

300 د. محمود نجيب حسني ، المرجع السابق ، ص517

قيام الجاني بإسناد فعل إلى المجني عليه ينصب على واقعة محددة تؤدي إلى عقاب المجني عليه أو احتقاره والأصل أن يكون القذف علنياً وفقا لما جاء في المادة 326 من قانون الجزاء العماني إلا أن المشرع عاقب على القذف غير العلني وفقا للمادة 328 من ذات القانون.

أما السب فهو خدش شرف الشخص واعتباره عمداً دون أن يتضمن إسناد واقعة معينه إليه[301]،وتقوم جريمة القذف والسب وفق هذا المفهوم بأي وسيلة من وسائل التعبير المختلفة ، قولية أو كتابية أو بالإشارة الدالة عليه، إلا أن المشرع العماني خصص القذف والسب الذي ينشر عبر وسائل تقنية المعلومات أو شبكة المعلومات الدولية فجرمه وفقاً للمادة 16 من قانون مكافحة جرائم تقنية المعلومات وهذا التخصيص تبعه تشديد في العقوبة حيث أن القذف وفق أحكام المادة (326) من قانون الجزاء العماني جريمة عقوبتها السجن مدة لا تقل عن شهر ولا تزيد عن سنة ، في حين أن السب عقوبته وفقاً للمادة (327) من ذات القانون وهي السجن لا تقل عن عشرة أيام ولا تزيد على سته أشهر، أما المادة 16 فقد شددت العقوبة الحبسية في حديها الأدنى والأعلى لتصل إلى السجن الذي لا يقل عن سنة ولا يزيد عن ثلاث سنوات.

الخاتمة :

تناولت هذه الورقة البحثية موضوع الأمن السيبراني وحرية الرأي والتعبير في وسائل التواصل الاجتماعي وفق القانون العماني ، بهدف بيان الحدود الفاصلة بين حرية التعبير عن الرأي في وسائل التواصل الاجتماعي والقيود الواردة عليها ، وتحديد المسؤولية الجزائية المترتبة على تجاوز تلك الحدود ، وخلصت هذه الورقة إلى الآتي :

1. حرية الرأي والتعبير حق دستوري كفله المشرع العماني للجميع ، وحرم المساس به وجرم أي اعتداء عليه، ولكل شخص الحق في التعبير عن رأيه بالوسيلة المناسبة، ومن تلك الوسائل مواقع التواصل الاجتماعي، والمنتديات الحوارية التي تستخدم شبكة المعلومات الدولية أو وسائل تقنية المعلومات .
2. حرية الرأي والتعبير المكفولة دستوريا بموجب النظام الأساسي للدولة ليست حرية مطلقة بل هي حرية مقيدة ، تقيدها حقوق الأخرين وحرياتهم والنظام العام للدولة ، فتقف حرية الرأي والتعبير عندما تمس بالنظام العام أو حريات الأخرين وحقوقهم .

301 د. عادل عبد إبراهيم العاني ، المرجع السابق ،ص313

3. تجاوز حدود حرية الرأي والتعبير في وسائل التواصل الاجتماعي من الجرائم السيبرانية المعاقب عليها وفق قانون مكافحة جرائم تقنية المعلومات كونها من جرائم المحتوى الرقمي .
4. هناك ارتباط وثيق بين الأمن السيبراني وحرية الرأي والتعبير، فكلما كان الأمن السيبراني مرتفع من خلال فاعلية القوانين وفاعلية السلطات المنفذة (تنفيذية ، وقضائية) كلما شكل ذلك ضمانة لحرية التعبير عن الرأي فتكون في إطار الحدود المكفولة دستورياً.
5. لا يعاقب القانون العماني عن الرأي المجرد الذي لم يخرج إلى العالم الخارجي بأحد وسائل التعبير عن الرأي ولو كان مضمون ذلك الرأي يتعلق بارتكاب جريمة من الجرائم المعاقب عليها وفق أحد القوانين العقابية بالسلطنة.
6. هناك التزم وتوازن تشريعي في القوانين العمانية فما نص عليه النظام الأساسي للدولة كحقوق دستورية ترجمته القوانين العقابية على شكل جرائم بهدف ضمان حماية تلك الحقوق من الاعتداء عليها .
7. شدد المشرع العماني العقوبة عندما ترتكب باستخدام شبكة المعلومات الدولية أو وسائل تقنية المعلومات ، لما تشكله تلك الوسائل من خطورة بالغة تتمثل في الوصول السريع والواسع للبيانات والمعلومات التي تنشر.

المراجع

أولاً: المراجع القانونية

1. د. أحمد عبدالرحمن شرف الدين ، مبادي القانون الإداري ، دار الفكر المعاصر ، الطبعة الأولى ، 2002
2. د.أحمد نهاد محمد الغول ، حرية الرأي والتعبير في المواثيق والتشريعات المحلية ، سلسلة تقارير قانونية (65) انظر C:/Users/User/Downloads/legal65%20(2).pdf
3. د. خالد مصطفى فهمي ، حرية الرأي والتعبير ، دار الفكر الجامعي ، الإسكندرية ط1، 2009.
4. د. داود الباز ، حماية السكينة العامة معالجة لمشكلة العصر في فرنسا ومصر الضوضاء ،دار الفكر العربي ، 2004
5. زهدي يكن ، القانون الإداري منشورات المكتبة العصرية ، صيد بيروت ، ط1 ، 1973 .
6. د . سليمان الطماوي ، الوجيز في القانون الإداري ، دار الشروق ، القاهرة ، 1967.
7. عبدالله محمد محمود ، المدخل إلى علم القانون أو النظرية العامة للقانون، ط7 ، مطبوعات جامعة دمشق ، 1996.
8. د.عبدالله خليل ، الحماية القانونية للصحفيين وأخلاقيات العمل الصحفي ، منشور على الصفحة الإلكترونية www.cdfj.org
9. عبد القادر عودة ، التشريع الجنائي الإسلامي مقارن بالقانون الوضعي ، مؤسسة الرسالة بيروت سوريا، ط3 ، 1994.
10. د . عادل عبد إبراهيم العاني ، شرح قانون الجزاء العماني القسم العام ، مكتبة الأجيال ، ط1، 2018م .
11. د عادل عبد إبراهيم العاني، شرح قانون الجزاء العماني القسم الخاص الجرائم الواقعة على الأشخاص و الأموال ، شركة مطابع الباطنة ومكتباتها للطباعة التكنولوجية الحديثة ، ط1 ، 2021 ،.
12. د. عثمان عبد الملك صالح ، حقوق الأمن الفردي في الإسلام ، دراسة مقارنة بالقانون الوضعي ، مجلة الحقوق .ع3/س7، 1983 .
13. عبد الواحد كرم ، معجم مصطلحات الشريعة والقانون ، دار المناهج ، الأردن ،ط2، 1998م.
14. د . غازي حسن صباريني ،الوجيز في حقوق الانسان وحرياته الأساسية ، دار الثقافة للنشر والتوزيع ، الأردن ، ط4، 2015 .
15. محمد الزجيلي ، حقوق الإنسان في الإسلام ، دار الكلم الطيب ، دمشق ، ط3، 2003.
16. فيصل نسيغة ، النظام العام ، بحث منشور في مجلة المنتدى القانوني العدد الخامس، جامعة محمد خيضر بسكرة، ، أنظر http://archives.univ-biskra.dz
17. د . محمود أبو السعود حبيب ، القانون الإداري ، دار الثقافة الجامعية ،ط1 ، 1999 .

18. د. محمد احمد فتح الباب السيد ، سلطات الضبط الإداري في مجال ممارسة حرية الاجتماعات العامة – رسالة دكتوراة جامعة عين شمس ، 1993 .
19. د. مجمود نجيب حسني ، شرح قانون العقوبات القسم العام ،ط6، دار النهضة العربية 1982،5،1989،ص 270-272
20. فاطمة طاهري ، القيم الدينية للثورة التحريرية الجزائرية كفكر وممارسة ، ملخص رسالة دكتوراه منشور على الموقع الالكتروني https://www.pnst.cerist.dz
21. د. مسفر بن حسن مسفر القحطاني ، الحماية المدنية للمعلومات الحاسوبية الشخصية(التعويض) في الفقه الإسلامي وأنظمة المملكة العربية السعودية ، مركز البحوث والدراسات بكلية الملك فهد الأمنية ،2005.
22. د. محمود نجيب حسني ، شرح قانون العقوبات ، القسم الخاص ـ جرائم الاعتداء على الأشخاص ، 1981م .
23. د. فوزية عبد الستار ، شرح قانون العقوبات القسم الخاص ، دار النهضة العربية ، القاهرة ،1982م .
24. نزار أيوب ، حرية الرأي والتعبير في مناطق السلطة الوطنية الفلسطينية ، دراسة مقارنة في ضوء المواثيق الدولية لحقوق الإنسان والتشريعات الفلسطينية ، رام الله مؤسسة الحق ، 2001.
25. يوسف القرضاوي ، الحلول المستوردة وكيف جنت على أمتنا ، دار البعث للطباعة والنشر ، قسنطينة ، ط1، 1984.

ثانياً : القوانين

1. النظام الأساسي للدولة الصادر بالمرسوم السلطاني رقم (2021/6) ،منشور في الجريدة الرسمية رقم 1374 .
2. قانون المطبوعات والنشر رقم(84/49)، منشور في الجريدة الرسمية رقم 289 ، الصادر بتاريخ 1984/6/2م
3. قانون الإجراءات الجزائية رقم (99/97).
4. قانون الجزاء العماني رقم(2018/7) .
5. قانون مكافحة جرائم تقنية المعلومات رقم(2011/12)، منشور في الجريدة الرسمية رقم (929) ، الصادر بتاريخ 2011 /2/15

ثالثاً: المواقع الالكترونية

1. أنظر الموقع الالكتروني WWW.radionongrata.og
2. انظر الموقع الالكتروني www.atheer.om
3. انظر الموقع الالكتروني HTTP://WWW.PHRMOVMENT.ORG/PDF/CHARTER

الأمن السيبراني والتحديات المُستقبلية

الدكتور أنور حاميم بن سليم
خبير ومحاضر دولي في الابتكار واستشراف المستقبل
مدير عام مركز الابتكار العالي بدولة الإمارات (بريطانيا)

مقدمة:

يستمر التهديد السيبراني العالمي في التطور بوتيرة سريعة، مع ارتفاع عدد انتهاكات البيانات كل عام فيما يخص الأمن السيبراني، وقد كشف تقرير صادر عن مؤسسة الأمن القائم على المخاطر عن تعرض ٧.٩ مليار سجل لانتهاكات البيانات في الأشهر التسعة الأولى من عام ٢٠١٩م وحده. هذا الرقم هو أكثر من ضعف عدد السجلات التي تم الكشف عنها في نفس الفترة من عام ٢٠١٨ م

وكانت جلسة عام ١٩٦٧م التي نظمها ويليس وير في مؤتمر الربيع المشترك للحاسوب والنشر اللاحق لتقرير المؤتمر لحظات تأسيسية هامة في تاريخ مجال الأمن السيبراني امتد عمل ويليس وير إلى تقاطع الاهتمامات السياسية والمادية والثقافية والاجتماعية

وفي عالم يعتمد على التكنولوجيا أكثر من أي وقت مضى ينتهج الأمن السيبراني الناجح نهجاً معيناً يتكون عادة من طبقات متعددة للحماية تنتشر في أجهزة الكمبيوتر أو الشبكات أو البرامج أو البيانات التي ينوي المرء الحفاظ على سلامتها، وفي أي دولة يجب على المستخدمين والعمليات والتكنولوجيا أن يكملوا بعضهم بعضاً، ويتكاتفوا لإنشاء دفاع فعال من الهجمات السيبرانية. ((من خلال تعاوننا معاً، سنتمكن من تحقيق التوازن بين الأمن والتنمية في عالم يزداد فيه الاعتماد على التقنيات الرقمية)) كين هو - رئيس مجلس الإدارة لشركة هواوي

المشكلة:

استهداف الأنظمة والشبكات والبرامج والمواقع بهجمات إلكترونية والوصول إلى المعلومات الحساسة بهدف تغييرها أو إتلافها أو ابتزاز الأموال من المستخدمين.

التعريف:

يعرف الأمن السيبراني بأنه حماية الأنظمة والشبكات والبرامج والموقع الجغرافي من الهجمات الرقمية ومن أي مشكلة أو عائق أو هجمات إلكترونية تحول دون أداء عملها

ايضاً هو حماية أجهزة الحاسوب وأنظمتها والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الضارة، ومن سرقة أو تلف برامجها أو بيانتها الإلكترونية.
يُعرف أيضًا باسم أمن تكنولوجيا المعلومات أو أمن المعلومات الإلكترونية أو أمن الحاسوب.

ويعتبر مفهوم الأمن السيبراني أوسع من أمن المعلومات، حيث يتضمن تأمين البيانات والمعلومات التي تتداول عبر الشبكات الداخلية أو الخارجية والتي يتم تخزينها في خوادم داخل أو خارج المنظمات من الاختراقات

وقد بات الأمن السيبراني سلاح استراتيجي بيد الحكومات والأفراد، وفي عصر التكنولوجيا أصبح للأمن السيبراني الدور الأكبر في صد ومنع أي هجوم إلكتروني قد تتعرض له أنظمة الدول المختلفة

فئات الأمن السيبراني:

- ✓ **أمن الشبكات:** هو ممارسة تأمين شبكات الحاسوب من المتطفلين سواء كانوا مهاجمين مستهدفين أو برامج ضارة.
- ✓ **أمن التطبيقات:** يركز على إبقاء البرامج و الأجهزة خالية من التهديدات. يمكن أن يوفر التطبيق المخترق الوصول إلى البيانات المصممة لحمايتها. يبدأ الأمان الناجح في مرحلة التصميم قبل نشر البرنامج أو الجهاز.
- ✓ **الأمن التشغيلي:** يشمل العمليات و القرارات الخاصة بمعالجة أصول البيانات و حمايتها. الأدوات التي يمتلكها المستخدمون عند الوصول إلى شبكة و الاجراءات التي تحدد كيف و أين يمكن تخزين البيانات أو مشاركتها كلها تندرج تحت هذه المظلة.

هجوم سيبراني:

تعرضت شركة «كاسيا» الأمريكية التي تزود العديد من الشركات بخدمة إدارة تكنولوجيا المعلومات والتي لديها أكثر من أربعين ألف عميل لهجوم إلكتروني تضمن مطالبة ما قد يزيد على ألف شركة تستخدم نظامها بدفع فدية، ما اضطُر سلسلة مخازن شهيرة في السويد إلى إغلاق مؤقت لجميع متاجرها في البلاد والبالغ عددها نحو 800.

وأعلنت شركة «كوب سويدن» السويدية أن الهجوم الإلكتروني شل أنشطتها التي تمثل نحو 20% من القطاع في البلاد ويناهز حجم مبيعاتها 1.5 مليار يورو. حيث انه يستغل هذا النوع من البرامج الثغرات الأمنية الموجودة لدى الشركات أو الأفراد ويقوم بتشفير أنظمة الكمبيوتر ويطلب فدية لإعادة تشغيلها.

وبالرغم ان الشركة اعلنت أن الهجوم اقتصر على «أقل من 40 من عملائها» في العالم، إلا أن هؤلاء العملاء يوفرون بدورهم خدمات لشركات أخرى ، وطال الهجوم «أكثر من ألف شركة» بحسب شركة «هانتريس لابز» المتخصصة بالأمن السيبراني.

مؤشر الأمن السيبراني العالمي:

تبوأت دولة الإمارات المركز الخامس عالميا بمؤشر الأمن السيبراني 2020 الصادر عن الاتحاد الدولي للاتصالات التابع للأمم المتحدة الذي يرصد التحسن في مستويات الوعي بأهمية الأمن السيبراني في 193 دولة حول العالم.

يقيس التقرير البنية التحتية في الأمن السيبراني لحوالي 194 دولة حول العالم بناء على خمسة محاور هي:

1. **الإجراءات القانونية**
2. **الإجراءات الفنية/التقنية**
3. **الإجراءات التنظيمية**
4. **إجراءات تطوير القدرات**
5. **إجراءات التعاون**

ويقيس كل محور من المحاور الخمسة 20 نقطة، حيث حققت دولة الدرجة كاملة في 3 محاور هي الإجراءات القانونية وتطوير القدرات وإجراءات التعاون، وحققت درجة إجمالية 98.06 من 100.

تقرير:

ظهر تقرير جديد أصدرته مؤسسة دبي للمستقبل بعنوان "الحياة بعد كوفيد-19: مستقبل الأمن السيبراني"، تزايداً ملحوظاً في الهجمات السيبرانية والجرائم الإلكترونية خلال الفترة الماضية، مع ظهور ثغرات أمنية في أنظمة البنى التحتية القائمة في ظل تفشي فيروس كورونا المستجد في مختلف دول العالم.

وأرجع التقرير الذي يأتي ضمن سلسلة التقارير التي تنشرها المؤسسة لاستشراف مستقبل القطاعات الحيوية، الزيادة في حجم التهديدات السيبرانية إلى سعي المخترقين المتواصل للوصول إلى المعلومات التي تجمعها الدول والحكومات لتتبع المصابين والحد من انتشار الفيروس، وتوظيفها في الهجمات الإلكترونية التي ينفذونها ما يضع أمن المعلومات أمام تحديات كبيرة.

واستعرض مجموعة من تقارير شركات متخصصة بأمن المعلومات كشفت عن تصاعد الجرائم الرقمية بنسب عالية، بما في ذلك تقرير صادر عن شركة مايم كاست، بعنوان «100 يوم من فيروس كورونا» ذكر أن عدد الجرائم الإلكترونية ارتفع بنسبة 33% منذ مطلع العام الحالي حتى نهاية مارس الماضي، مع ازدياد عدد زيارات الروابط غير الآمنة أكثر مما كان قبل تفشي الوباء.

وأشار إلى أن رسائل البريد الإلكتروني المخادعة زادت أكثر من 600% منذ شهر فبراير الماضي، حيث استهدف المخترقون الأشخاص والمؤسسات من خلال الروابط المشبوهة واختراق البريد الإلكتروني للحصول على بيانات الدخول إلى الحسابات المالية، وأنشأوا أكثر من 100 ألف نطاق جديد لمواقع إلكترونية عن كوفيد-19 في محاولة لخداع الأفراد كي يسجلوا بياناتهم.

زيادة البرمجيات الخبيثة في المنطقة

ورصدت "مايم كاست" زيادة ملموسة في البرمجيات الخبيثة والبريد "الإغراقي" في الدول العربية، وذكر أحد مسؤوليها أن الشركة رصدت حدوث ارتفاع بنسبة 751% في زيارة الروابط غير الآمنة خلال الأشهر الثلاثة الأولى من تفشي الفيروس، ما يعني تخلي الناس عن حذرهم مقابل رغبتهم في معرفة معلومات إضافية عن الفيروس سواء كانت حقيقية أم زائفة.

لماذا تراجع مستوى الأمن السيبراني؟

وأشار التقرير إلى أن التوجه العالمي لاعتماد الأنظمة التعليمية والصحية والحكومية والخاصة على الحلول الرقمية أتاح للمخترقين أعداداً هائلة من الأهداف التي أصبحت تحت رحمة هجماتهم، خاصة أن معظمها لم يخطط مسبقاً للتحول الرقمي بهذه السرعة، ولم يختبر مستوى أمن نظمه الرقمية.

أهم القطاعات المستهدفة

ولاحظ التقـــرير أن قطاع الرعايـــــة الصحية يأتي على رأس القطاعات التي تعرضت للهـــجمات السيبرانية من خلال هجمات برامج الفدية، خصوصا أن مرتكبـــي الهجمات الإلكترونية كانـــوا يعتقدون أن المؤسسات الصحية ستضطر إلى دفع الأمـــوال "الفدية" لاستعادة أنظمتها التي تعتمد عليها في مواجهة انتشار الفيروس.

وبين التقرير أن أعداداً كبيرة من المخترقين يستغلون أزمة الفيروس لبيع الأدوات الطبية المزيفة، وانتحال شخصيات لمسؤولين حكوميين ونشر ادعاءات بالتوصل إلى علاجات جديدة للفيروس والترويج لمنتجات طبية وهمية بملايين الدولارات.

وكان القطاع المالي والنفطي في المرتبة الثانية للأهداف المفضلة للمخترقين، وأشار التقرير إلى تحذير المصارف المركزية من المحتالين الذين يسعون لاختراق الحسابات المصرفية، فيما يعد قطاع النفط من الأكثر تأثراً في منطقة الشرق الأوسط وشمال إفريقيا، إذ تعرضت شركاتٌ عديدة لرسائل بريد إلكتروني مخادعة، بهدف الحصول على تفاصيل ومعلومات عن الأفراد وعمليات إنتاج النفط، كي يبيعوها بعد ذلك على "الإنترنت المظلم."

منصات الفيديو والألعاب الإلكترونية

كما تعد منصات مؤتمرات الفيديو من أهم الأهداف المفضلة للمخترقين، إذ ظهرت فيها بعض الثغرات الأمنية، مثل منصة "زوم" التي شهدت انضمام بعض الأشخاص عشوائياً إلى اجتماعات الفيديو وتعطيله بمحتوى غير مرغوب به، أو نشر فيديوهات مسجلة لم يتم حفظها في مساحات تخزين سحابية آمنة، وتم نشرها بعد ذلك على شبكة الإنترنت وشمل ذلك اجتماعات عمل خاصة، ومحادثات شخصية بين عائلاتٍ وأصدقاء، وتعرضت أيضاً منصاتٌ أخرى مثل منصات الألعاب عبر الإنترنت إلى هجماتٍ سيبرانية بهدف اختراق شبكة "نينتندو" للحصول على معلومات مالية شخصية.

إعادة تقييم الاستراتيجيات والنظم الأمنية

وأشار التقرير إلى ضرورة مبادرة الجهات الحكومية والشركات الخاصة لإعادة تقييم استراتيجيات الأمن السيبراني وسياسات أمن شبكة الإنترنت لمواجهة هذه المخاطر، حيث عملت بعض الشركات على تعزيز أنظمتها الحالية، حيث أصدرت "جوجل" و"آبل" بياناً تؤكد فيه للمستخدمين أن نظامهم لتتبع الاتصال سيُشفر، وأن اتصال بلوتوث المستخدم لتتبع الموقع سيكون قوياً إلى درجة كافية كي لا يُخترق لتحديد الموقع والحصول على تفاصيل الجهاز.

وتطرق التقرير إلى استخدام تقنيات جديدة لتطوير منصات الأمن السيبراني الحالية، إذ تبحث العديد من المراكز العالمية في كيفية استخدام الذكاء الاصطناعي لمواجهة التهديدات السيبرانية. ومنها تعلم الآلة لتحليل مجموعات البيانات وتحديد الأنماط والصلات الخاصة بالهجمات بسرعة أكبر مما يمكن أن يفعله المحققون باستخدام الوسائل التقليدية.

توقعات وتوصيات في التقرير

وخلص التقرير إلى عدد من الرؤى والتوصيات بشأن مستقبل حماية المعلومات الرقمية من الهجمات الإلكترونية الخبيثة لتعزيز الأمن السيبراني، وضمان أمن المعلومات والبيانات، ومواجهة تحديات قراصنة المعلومات لفضاء إلكتروني أكثر أمناً.

ورأى أن عمل موظفي أمن تقنية المعلومات عن بُعد، وانخفاض قدرتهم على اكتشاف الهجمات الإلكترونية بكفاءة قد يتطلب تطبيق تدابير جديدة، ولتفادي هذه المخاطر ستبدأ الهيئات الحكومية دراسة استخدام أنظمة الأمن الإلكتروني التي تعتمد على الذكاء الاصطناعي لتوفير التحليل المستمر للتهديدات السيبرانية والهجمات المحتملة، فيما سيصبح التطبيب عن بعد أحد أساليب الرعاية الصحية، لكن لا بد من إقرار إرشادات موحدة لكيفية إعداد الأجهزة الطبية وتشغيلها.

وتوقع التقرير أن يزداد ذكاء الهجمات الإلكترونية من المخترقين مع الزمن وأن تزداد صعوبة مكافحتها كلما تطورت التقنية، وأوضح أنه مع زيادة تبني استخدام الأتمتة في المستقبل سيراقب المبرمجون ومطورو المنتجات، الأنظمة وهي تعمل وتقاوم الهجمات دون تدخلٍ منهم، وسيؤدي هذا إلى وجود قطاع أمن إلكتروني عالمي يقوده الذكاء الاصطناعي

نموذج من أوروبا:

وضعت المفوضية الأوروبية ما أسمته بــ" البوصلة الرقمية"، وهي مصفوفة أهداف خاضعة للتقييم بحلول العام 2030، والتي تقوم على مجموعة أهداف مرحلية، هي:

- **التحول الرقمي للأعمال :** يجب أن تستخدم ثلاث شركات من أصل أربع خدمات الحوسبة السحابية والبيانات الضخمة والذكاء الاصطناعي، وأن تصل أكثر من 90% من الشركات الصغيرة والمتوسطة الأوروبية إلى مستوى أساسي على الأقل من الكثافة الرقمية، مقارنة بـ 61% في عام 2019. كما يجب أن يكون هناك حوالي 250 شركة يونيكورن (شركات ناشئة بقيمة مليار دولار) في الاتحاد الأوروبي، بزيادة 100% مقارنة بعام 2021.

- **بُنى تحتية رقمية مستدامة وآمنة وفعالة :** يجب أن يكون لدى جميع الأسر الأوروبية اتصال سريع على الإنترنت مقارنة بـ 59% في عام 2020، وسيتم تغطية جميع المناطق المأهولة بواسطة الـG5 ، بزيادة من 14% في عام 2021، وأن يمثل إنتاج أشباه الموصلات المتطورة والمستدامة في أوروبا، بما في ذلك المعالجات، 20% على الأقل من قيمة الإنتاج العالمي، وأن يتضاعف من 10% في عام 2020. كما يجب نشر 10000 عقدة حافة محايدة مناخياً عالية الأمان (والتي ستسمح بمعالجة البيانات على حافة الشبكة) في الاتحاد الأوروبي، وتوزيعها بطريقة تضمن الوصول إلى البيانات بزمن انتقال منخفض. كما يجب أن يكون لدى أوروبا أول حاسوب كمومي (Quantum computing) بحلول العام 2025.

- **الخدمات العامة للرقمنة :** يجب أن تكون جميع الخدمات العامة الرئيسة متاحة على الإنترنت، وتمكين جميع المواطنين من الوصول إلى سجلاتهم الطبية الإلكترونية، فيما يجب أن يستخدم 80% من المواطنين حلول الهوية الرقمية.

- **السكان ذوو المهارات الرقمية، والمهنيون الرقميون ذوو المهارات العالية :** يجب أن يتمتع 80% على الأقل من جميع البالغين بالمهارات الرقمية الأساسية. كما يجب أن يكون هناك 20 مليون متخصص في تكنولوجيا المعلومات والاتصالات في الاتحاد الأوروبي مع تقارب بين النساء والرجال، مقارنة بـ 7.8 مليون في عام 2019[3].

نموذج من دولة الإمارات العربية المُتحدة:

اتخذت دولة الإمارات العديد من الإجراءات والتدابير والمبادرات لتعزيز أمنها السيبراني بتولي فريق الشبكة الإلكترونية الاتحادية مهمة رصد ومراقبة وقائع ومجريات البنية التحتية للشبكة الإلكترونية الاتحادية على مدار الساعة، بما يضمن اتخاذ الإجراءات اللازمة في حال حدوث أخطاء أو انتهاكات

وتعمل دولة الإمارات على تعزيز الأمن الرقمي لأفراد المجتمع من مواطنين ومقيمين من خلال عدة مبادرات تشمل بطاقة الهوية الصادرة من دولة الإمارات، وإطلاق تطبيق الهوية الرقمية (**تطبيق الهوية الرقمية** **UAE Pass app**) تعد الهوية الرقيمة أول هوية وطنية رقمية لجميع المواطنين والمقيمين والزوار، وتسمح بوصول المستخدمين إلى خدمات الهيئات الحكومية المحلية والاتحادية، ومزودي الخدمات الآخرين. تقدم الهوية الرقمية أيضاً حلولاً سهلة للدخول إلى الخدمات عبر الهواتف الذكية دون الحاجة إلى كلمة سر أو اسم مستخدم، فضلاً عن إمكانية التوقيع على المستندات رقمياً، والتحقق من صحتها دون الحاجة لزيارة مراكز الخدمة.

إطلاق مؤشر دبي للأمن الإلكتروني الأول من نوعه على مستوى العالم، والذي يدعم الأداء العام للأمن الإلكتروني في مختلف الجهات الحكومية على مستوى الإمارة، بما يرسخ مكانتها بوصفها المدينة الأكثر أمانا في الفضاء الإلكتروني، يأتي إطلاق المؤشر في إطار مستهدفات استراتيجية دبي للأمن الالكتروني لحماية إمارة دبي من مخاطر الفضاء الالكتروني، ودعم الابتكار والنمو الاقتصادي للإمارة في ظل التقدم التكنولوجي والتحول الذكي الذي تشهده ، حيث يتيح المؤشر تعزيز المنافسة بين الجهات الحكومية في مجال الأمن الإلكتروني وتطوير مقدراتها وتقدمها في هذا المجال.

وبموجب الإحصائيات، 87% من الأطفال يقضون اوقاتهم على الإنترنت و 34 من الأباء والأمهات يتركون أبنائهم يتصفحون دون الإشراف عليهم و 31% من الأباء والأمهات يعانون من التنمر على أبنائهم و 66% من الاباء والأمهات لا يقومون بتحديد الصلاحيات لأجهزة أبنائهم أطلقت وزارة الداخلية والبرنامج الوطني للسعادة وجودة الحياة المبادرة المشتركة "السلامة الرقمية للطفل" الهادفة إلى توعية الأطفال وطلاب المدارس بتحديات العالم الرقمي وتشجيعهم على استخدام الإنترنت بشكل إيجابي وآمن، وتوعية وتأهيل المعلمين والأهالي بأساليب مواجهة هذه التحديات بما يحقق السلامة الرقمية لأطفالهم، وتشمل مبادرة "السلامة الرقمية للطفل"

تطوير موارد تعليمية حول السلامة الرقمية، وتمكين الأطفال من أفضل الممارسات العالمية في هذا المجال، وتعريف الآباء والمعلمين بآليات تعزيز السلامة الرقمية للأطفال في المنازل والمجتمع المدرسي.

إطلاق منصة صنّف لتقييم محتوى الألعاب الإلكترونية تتيح منصة صنف لأولياء الأمور التعرف إلى الألعاب الإلكترونية ومحتواها وطبيعتها، قبل عرضها على الأطفال، حيث تقدم المنصة إمكانية البحث عن أي لعبة إلكترونية، وإظهار المخاطر التي قد تحتوي عليها، ما يساعد ولي الأمر على اختيار الألعاب الأنسب لأبنائه.

إطلاق المنصة المعرفية لجودة الحياة الرقمية والتي تشكل بوابة إلكترونية تشتمل على محتوى توعوي لبناء القدرات الرقمية خصوصاً الطلبة وأولياء الأمور والمعلمين، وأصحاب الهمم وكبار المواطنين.

تنفيذ وإطلاق شبكة إلكترونية اتحادية (FEDNET) تسمح بالتوصيل البيني، وتبادل البيانات بين جميع الجهات المحلية والاتحادية في الدولة، وتعزز قنوات التواصل فيما بينها باستخدام بنية تكنولوجية موحدة وآمنة.

توفر الشبكة بيئة أمن متعددة الطبقات تضمن أعلى مستويات الأمان في البنية التحتية اعتماداً على الترميز متعدد البروتوكولات (MPLS) وتتيح ربطاً آمناً بالإنترنت لكافة الجهات الحكومية الاتحادية عبر مزود مزدوج لخدمة الإنترنت، ما يسمح بتحقيق إنتاجية أعلى. كما توفر هذه الخدمة اتصالاً موحداً بالإنترنت في الجهات الاتحادية، مما يقلل إمكانية التعرض لهجمات الدخلاء عن طريق الحد من الثغرات، كما يتولى فريق الشبكة الإلكترونية الاتحادية مهمة رصد ومراقبة وقائع ومجريات البنية التحتية للشبكة الإلكترونية الاتحادية على مدار الساعة، بما يضمن اتخاذ الإجراءات اللازمة في حال حدوث أخطاء أو انتهاكات بغض النظر عن مستواها.

تحديات يجب الاستعداد لها:

- **الأمان والخصوصية:** تواجه مشاريع التحول الرقمي في العالم – معضلتي الأمان والخصوصية، حيث ستعتمد معظم الأنشطة اليومية على الخدمات عبر الإنترنت: من إدارة المستشفيات إلى شبكات الكهرباء والخدمات المالية إلى تخزين المعلومات الخاصة. ويمكن أن تؤدي الهجمات الإلكترونية والبرمجيات الخبيثة والحوادث العرضية (مثل قطْع الكابلات في أعماق البحار أو حملات التشويه على وسائل التواصل الاجتماعي) إلى تعريض أداء بلدان بأكملها للخطر.

- **صعود الاقتصاد غير الحقيقي:** سيؤدي التحول الرقمي العالمي إلى صعود الاقتصاد الرقمي مقابل انخفاض الاقتصاد الحقيقي، بسبب إقبال الشركات على العمل في القطاع الرقمي بحثاً عن الحوافز، فالاقتصاد الرقمي يحتاج إلى رأس مال أقل بكثير للتطور، وبالتالي يمكنه التوسُّع بشكل أسرع مقارنة بالصناعات التقليدية. كما أن العصر الرقمي يجعل الأسواق متعددة الجوانب هي القاعدة، وليس الاستثناء، حيث "العملة" في المعاملات ليست المال بل البيانات، البيانات التي يمكن تحويلها إلى معلومات، والتي أصبحت تسمى "نفط القرن الحادي والعشرين، مما قد يؤثر على قطاع الإنتاج التقليدي الصناعي والزراعي والخدمي، ويمكن أن يجعل كثير من الدول في تبعية اقتصادية للقوى المنتجة عالمياً، وخاصة الصين الباحثة عن أسواق جديدة لفوائض إنتاجها.

- **تحديات صناعة الطيران:** تعتمد صناعة الطيران بشكل كبير على سلسلة من الأنظمة المعقدة التي يمكن مهاجمتها. يمكن أن يتسبب انقطاع التيار الكهربائي البسيط في أحد المطارات بحدوث تداعيات في جميع أنحاء العالم، ويعتمد جزء كبير من النظام على عمليات الإرسال اللاسلكي التي يمكن أن تتعطل، كما أنَّ التحكم في الطائرات فوق المحيطات أمر خطير بشكل خاص لأن مراقبة الرادار تمتد فقط من ٢٨٠ إلى ٣٦٠ كيلومتر في الخارج. هناك أيضًا إمكانية للهجوم من داخل الطائرة وبالتالي مخاطر أعلى للأمن السيبراني كنظام متكامل.

- **القطاع الحكومي:** عادة ما تتعرض أنظمة الحاسوب الحكومية و العسكرية للهجوم من قبل المخربين و القوى الأجنبية أو المحلية. البنية التحتية الحكومية المحلية و الإقليمية مثل ضوابط إشارات المرور، و اتصالات الشرطة، و وكالات الاستخبارات، و سجلات الموظفين، و الأنظمة المالية هي أيضًا أهداف محتملة لأنها أصبحت الآن جميعها محوسبة إلى حد كبير. يمكن أن تكون جوازات السفر و بطاقات الهوية الحكومية التي تتحكم في الوصول إلى المرافق عرضة للاستنساخ أيضاً من خلال تهديد الأمن السيبراني للدولة أكملها ممثلة بحكوماتها.

وغيرها من التحديات في المجال البيئي والمجال الصناعي والمعدات والمحركات وغيرها

نصائح حول الأمن السيبراني:

<u>تحديث</u> البرامج و أنظمة التشغيل الخاصة وذلك للاستفادة من أحدث تصحيحات الأمان المتوفرة ، **<u>استخدام</u>** برامج مكافحة الفيروسات وذلك لاستكشاف الحلول الأمنية و التهديدات و إزالتها من خلال النظام

المعمول به ، **المحافظة** على تحديث البرامج للحصول على أفضل مستوى من الحماية ، **استخدام** كلمات مرور قوية والتأكد من عدم سهولة تخمين كلمات المرور ، **عدم النقر** على الروابط الموجودة في رسائل البريد الإلكتروني من مرسلين غير معروفين أو مواقع غير مألوفة ،**عدم فتح** مرفقات البريد الإلكتروني من مرسلين غير معروفين وذلك لأنها قد تكون مصابة ببرامج ضارة، **تجنُب** استخدام شبكات الواي فاي غير الآمنة في الأماكن العامة لأنها قد تكون عرضة للهجوم على مستوى الهجمات المتوسطة و ربما الأكثر ضرراً أيضا.....

ختاماً نسأل الله ان يُجنبكم و يُجنب جميع الدول من الأضرار والإختراقات وكل ما يُقلق امنها وإستقراراها.

كيفية مساهمة شركات التقنية في تسهيل عمليات الاختراق الالكتروني

الدكتور عبيد صالح المختن،
باحث وأكاديمي في تقنية المعلومات والجريمة الالكترونية (الإمارات)

الملخص:

ان التطور الكبير والمتسارع في تقنيات المعلومات والاتصال سمة من سمات هذا العصر ولا يمكن وقف هذا التطور او الاختباء او رفضه، فالأمن السيبراني يعرف بأنه حماية كل الكيانات الوطنية الالكترونية والمعلوماتية من الاعتداء او التغيير او التعديل، وما نحاول ان نبرزه في هذه الورقة ان التوسع الكبير في استخدام هذه التقنيات ودخوله في كل المجالات وسهولة جمع البيانات الدقيقة عن سلوك البشر والمجتمعات وخضعها للدراسة والتحليل ودمجها في مشاريع دون علم الدول او حتى الاشخاص اصحاب هذه البيانات، فتتكشف لنا جوانب سلبية لها تأثير قد يكون مدمرا ويهدد كيان الدول واستقرارها وحتى السلم والامن العالمي، فيجب حصر جوانب الاختلال التي قد تعصف بهذا الكيان الافتراضي فهنا يجب الالتفات لهذه الكيانات الوسطية والتي تمارس الاعمال الخارجة عن نطاق القانون والتي وفرتها هذه التقنيات وتتحكم بها وتديرها وتعد جوانبها الامنية والقانونية، فهي مسؤولة بما يدور في هذا الفضاء الالكتروني سواء من عوامل ايجابية او سلبية، وما تعرضنا له من توصيات تصب في مصلحة اعادة سيطرة مؤسسات وطنية وامنية على هذه التطبيقات وايجاد كيان يهتم بالمحافظة على البيانات البشرية ومنع وصول أي جهات اخرى لها ومحاسبة هذه الكيانات الوسطية عن أي خلل او تعدي.

Summary:

The great and accelerating development in information and communication technologies is a feature of this era and this development cannot be stopped, hidden or rejected. Cyber security is defined as protecting all national electronic and informational entities from attack, change or modification. In the use of these technologies and its entry into all fields, and the ease of collecting accurate data on the behavior of humans and societies, subjecting them to study and analysis, and integrating them into projects without the knowledge of countries or even the people who own this data, then we discover negative aspects that have an impact that may be devastating and threaten the entity and stability of countries and even global peace and security. The aspects of disruption that may afflict this virtual entity must be limited. Here, attention must be paid to these intermediate entities that engage in activities outside the scope of the law, which these technologies provide, control and manage, and consider their security and legal aspects, The recommendations we have presented are in the interest of restoring the control of national and international institutions over these applications and finding an entity concerned with preserving human data, preventing access to it by any other parties, and holding these intermediate entities accountable for any defect or infringement.

المقدمة

ان التطور الكبير والمتسارع في تقنيات المعلومات والاتصال سمة من سمات هذا العصر حيث اضحت هذه التقنيات هي مفتاح الحلول للكثير من المشكلات المزمنة والعلاجات لكثير من الامراض واصبحت هي افضل الحلول للتصدي للأوبئة وضمان استمرارية الاعمال ولا يستطيع أي احد ان ينكر فضل الانترنت للمساهمة في التخفيف من اثار جائحة كورونا فهي كانت خيل السبق الفائز لكل دولة استثمرت في البنية التحية واتسعت في استخدام الخدمات الحكومية الإلكترونية والذكية والعمل والدراسة عن بعد، في المقابل نجد في الجانب المقابل تفشي ظاهرة الاستخدام غير الشرعي للفضاء الرقمي في ظل معادلة تُزاوج غير شرعي بين تكنولوجيا المعلومات والإرهاب حيث امسى امتلاك اسرار هذه التقنيات هي ميزة وسلاح استراتيجي بالغة الأهمية، وبدأت بعض من انماط الارهاب الدولي بالتكشف ممثلة في الارهاب الالكتروني او السيبراني حيث يعرف بانه عبارة عن عدوان او تخويف او تهديد مادي أو معنوي على الإنسان، في دينه، أو نفسه، أو عرضه، أو عقله، أو ماله بغير حق، باستخدام الوسائل التقنية، وكان لابد المجتمع الدولي التصدي لهذا النوع من الافساد والاضرار بإنشاء وحدات وهيئات تحد من وصول هذا الارهاب او تأثيراته وذلك باستخدام مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الوصول غير المصرح به، بهدف حماية وحفظ وضمان توافر واستمرارية عمل نظُم المعلومات، وتعزيز حماية وسرية وخصوصية البيانات الشخصية، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني.

تشير الاحصائيات العالمية الى انتشار الانترنت لدى سكان البشرية حيث ان هناك اكثر من 50% من البشر يستخدمون الانترنت وان 42% منهم متواجدون في برامج التواصل الاجتماعي وهناك اكثر من 2 مليار لاعب في الفضاء الالكتروني ومع زيادة مستمرة وان فضاءات التواصل الاجتماعي هي افضل مكان للايقاع بضحايا جدد، مما اعطى الجماعات المخربة ميزة كانت مستحيلة قبل انتشار الانترنت وهي الوصول لجميع فئات المجتمع في أي وقت يريدون ونشر افكارهم وايجاد اتباع والتخفي وجمع الاموال وكذلك التخطيط لعمليات تروع المجتمع بدون خوف او حذر من الإيقاع بهم من أجهزة الضبط القضائي، ومن خلال تحليل الهجمات الالكترونية سواء على الدول او المؤسسات او الافراد نجد ان هناك مساهمة من الشركات المصنعة لهذه البرامج والمشرفة عليها في اهمال اغلاق بعض الثغرات الأمنية مع اثبات اخطارها العديد من المرات مثلما حدث في الهجوم الشاسع في 2017 الونكراي حيث تسببت ثغرة في نظام التشغيل ويندوز في تسهيل وصول المخترقين للأجهزة والمطالبة بفدية مقابل الافراج عن بياناتهم المؤسسية والشخصية،

مشكلة الدراسة:

كلما تطورت التكنولوجيا وتوسع المستخدمون من دول ومؤسسات وافـــراد في استخداماتها والاعتماد عليها في كل مفاصل الحياة حيث اصبحت هذه التقنيات بكل ما تقدمــه من حلول هيه الحامي والحارس للمنظومة الالكترونية وبين فترة واخرى يتم الاعلان عن ثغرات امنيـــة تسببت في هجــــمات الكترونية تسببت في خسائر فادحة، ما نريد ان نوضحه في هذه الورقة ان نضـــع هذه الشـــركات التقنـــية كطرف ثالث في هذه الهجمات وحول المسؤولية الجنائية في اهمال الاغلاق التام لهذه الثغرات وبيـــن ما تجمعه من بيانات وتسهل لطرف آخر الحصول عليه تساهم في ارتكاب جرائم سيبرانية من تهديد وابتزاز وانتهاك الملكية الفكرية.

أولا مفهوم الامن السيبراني:

عرف ريشارد كمرر (Richara A.Kemmerer) الامن السيبراني بأنه:

"عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة"، اما إدوارد أموروسو (Edward Amoroso) عرف الامن السيبراني بأنه" وسائل من شأنها الحد من خطر الهجـــوم على البرمجيات او أجهزة الحاسوب او الشبكات، وتشمل تلك الوسائل المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها وتوفير الاتصالات المشفرة[302].

ووضحت وزارة الدفاع الامريكية تعريفا للامن السيبراني بأنه "جميع الاجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع اشكالها المادية والالكترونية من مختلف الجرائم والهجمات والتخريب والتجسس والحوادث[303].

تعرف دولة الامارات الامن السيبراني بأنه " بأنه حماية الأنظمة والشبكات والبرامج والموقع الجغرافي من الهجمات الرقمية، ومن أي مشكلة أو عائق أو هجمات إلكترونية تحول دون أداء عملها. وتهدف الهجمات الإلكترونية عادة إلى الوصول إلى المعلومات الحساسة بهدف تغييرها أو إتلافها أو ابتزاز الأموال من المستخدمين. ويعتبر مفهوم الأمن السيبراني أوسع من أمن المعلومات، حيث يتضمن تأمين البيانات والمعلومات

---

[302] **عنترة بن مرزوق، محي الدين حرشاوي, الامن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، جامعة القاصدي مرباح الجزائر،**

https://www.univ-ouargla.dz/index.php

[303] **Cybercrime Laws of the United States, https://www.oas.org/juridico/spanish/us_cyb_laws.pdf**

التي تتداول عبر الشبكات الداخلية أو الخارجية، والتي يتم تخزينها في خوادم داخل أو خارج المنظمات من الاختراقات[304].

ثانيا صور الجرائم السيبرانية:

تختلف الجريمة الاعتيادية والتي تقلصت بشكل كبير لتحل محلها الجريمة السيبرانية ولكن بشكل جديد ومميزات جديدة ومن صور الجريمة السيبرانية[305]:

1. الاعتداء على اجهزة الحاسب الالي
2. الاعتداء على حرمة الحياة الخاصة
3. الاعتداء على حقوق الملكية الفكرية
4. الاستيلاء والنصب والاحتيال السيبراني
5. الانتحال والتغرير السيبراني
6. الابتزاز والتهديد السيبراني
7. التنصت السيبراني
8. السطو الالكتروني على اموال البنوك
9. الاعتداء السيبراني على الاخلاق والاتجار بالبشر والمخدرات
10. الاعتداء السيبراني على الامن
11. تعطيل المصالح الحكومية

ثالثا تقنيات ساهمت في شيوع الجريمة السيبرانية

الانترنت مع بداية ظهوره اخذ بالتطور والانتشار بشكل كبير ولكن مازال الانترنت يخفي به جانب كبير من الظل والخفاء فالجزء الواضح من الانترنت والذي يحرك التجارة ووتتم فيه عمليات الاتصال والتواصل بين مختلف البشر والمؤسسات ومحركات البحث التي تجيب عن استفساراتنا لا يمثل سوى جزء ضئيل من

---

[304] **فاطمة عبدالله الدربي, مقالة بعنوان ما هو الامن السيبراني منشورة بجريدة البيان الاماراتية بتاريخ 13 يناير 2021،**
https://www.albayan.ae/opinions/by-the-way/2021-01-13-1.4064590

[305] **روان بنت عطية الله الصحفي دراسة منشورة بعنوان الجرائم السيبرانية منشورة بالمجلة الالكترونية الشاملة متعددة التخصصات، العدد الرابع والعشرون لشهر 5 2020، عمان، الأردن 2020، ص17-ص21**

حجم الانترنت الكبير وهناك جزء كبير من الانترنت لا تصله عين العدالة ولا يخضع لاي قوانين سوى المصلحة، فيقسم الانترنت الى:

1) انترنت السطحي Surface Web بدء من اول صفحة الكترونية أنشأت في عام 1991 الى ان اصبح اليوم هناك ما يقارب 1.8 مليار موقع الكتروني بمختلف لغات واهتمام الناس حول العالم تؤدي مختلف من الخدمات منها التواصل بين البشر والبريد الإلكتروني والبيع والشراء والتعليم ومواقع المكتبات والمراكز البحثية ومراكز الاخبار ووكالات الانباء وموقع الوكالات المتخصصة وكذلك الصفحات الشخصية[306]. الانترنت العميق Deep Web والدارك نت DarkNet وتستخدم فيه عملة رقمية خاصة تسمى البتكوين Bitcoin.

2) الانترنت العميق Deep Web هو مجموعة من المواقع الموجودة على شبكة الأنترنت لا يتم أرشفتها في جوجل ولن تجدها في نتائج البحث لأنها غير معروفة ا يمكن الوصول إليها بواسطة محركات البحث التقليدية، والبعض يقول انه يمكن تصل مساحة الـ Deep Web من اجمالي الإنترنت ما تعادل 85% في حين أن بعض التقديرات تضع حجم Deep Web بحجم 4000-5000 مرة أكبر من الويب السطحي وأن شبكة الويب العميقة تنمو بشكل كبير مما يشكل خطرا على النظام والسلم العالمي[307]، من خصائص صفحات مواقع الويب العميق:

- الصفحات اليتيمة: هي الصفحات التي لا توجد روابط إليها في صفحات أخرى
- صفحات ذات الوصول المحدود: هي الصفحات التي تمنع عناكب البحث من الوصول للمحتوى ببرامج التحقق من الروبوتات مثل الكابتشا.
- الصفحات غير النصية: هى الصفحات الغير قابلة للفهرسة والتى تحتوى على صيغ ملفات غير نصية مثل الفيديو والصور والـ pdf وغيرها من الصيغ الغير قابلة للأرشفة.
- الملفات المستضافة على بروتوكولات أخرى: مثل ftp وهى مواقع متواجدة لكنها تستخدم بروتوكولات خاصة ونطاقات خاصة ومتواجدة بشكل كبير ويصعب تعقبها أو التجسس عليها.

---

[306] موقع https://www.internetlivestats.com/ يختص بتقديم احصائيات لحظية عن الانترنت حول العالم.

[307] Bright Planet, Deep Web: A Primer, http://www.brightplanet.com/deep-web-university-2/deep-web-a-primer/.

3) الانترنت المظلم Dark web أو الـ Net Dark: هي شبكة داخلية من شبكة Web Deep، وسميت بهذا الأسم لكونها تحتوي على أنشطة غير قانونية مثل تجارة المخدرات والسلاح والتجارة في البشر، والشرط الأساسي لاستخدام الإنترنت المُظلم هو تشفير الهوية وعدم معرفة الشخص الذي يتصفح الإنترنت، وتصل مساحتها إلى 3% على شبكة الأنترنت[308].

4) عملة البيتكوين Bitcoin ويرمز لها BTC وهي عملة رقمية إلكترونية يتم تداولها عبرالإنترنت فقط، أسسها شخص مجهول عام 2007 ، وبدأ التعامل بها في عام 2009، تعمل دون وجود فيزيائي لها مشفرة لا مركزية ، أي تعمل دون مستودع مركزي او هيئة تنظيمية مركزية تقف خلفها وتتم المعاملات بشبكة الند للند بين المستخدمين مباشرة دون وسيط دون رقابة حكومية على طبيعة الانشطة او المواد المشتراة والمباعة فهي تستغلها اغلب العصابات في الانترنت المظلم في اخفاء انشطتها وحجم المبالغ المتحصل عليها مقابل انشطتها غير المشروعة[309].

5) الخير والشر تحدي منذ خلق الله الانسان وتتضح فجوة يستغلها المخربون بما تقدمه التقنية من تسهيلات وما تستطيع المؤسسات والافراد استخدامه وتطويعه للاستخدام فكلما استطاع المخربون الوصول الى منافع التقنية قبل الأجهزة المسؤولة عن التأمين عم الخراب التقني وزادت الهجمات السيبرانية ولو استطاع المختصين بالتأمين من الوصول الى منافع التقنية قبل المخربون واغلقوا كل الفرص امام كل مخرب ومن هذه الفرص التي يمكن المنافسه بين من يقوم بالتأمين والمخربين:

- تطور الأجهزة الحاسوبية (الأجهزة الكمية) فهي الالاف الاضعاف من السرعات وبالتالي تستطيع فكر الشفرات القديمة المكونة من حروف وارقام
- تطور سرعات الانترنت الجيل السادس G6
- انتشار الانترنت والتواصل الاجتماعي 40% من ضحايا الانترنت يتم الإيقاع بهم في منصات التواصل الاجتماعي فهي البيئة الخصبة للايقاع بالضحايا، وهنا يلعب عامل الوعي دورا أساسيا في وقف طرق الاستهداف والاحتيال.

[308] Michael Chertoff (2017) A public policy perspective of the Dark Web, Journal of Cyber Policy, 2:1, 26-38

[309] موقع https://bitcoin.org/ar/ البتكوين الرسمي تاريخ الزيارة 2021/07/22

- التساهل الأمني في سبيل التميز المؤسسي وكسب رضا العملاء وهنا يأتي دور الفرق المتجانسه في المؤسسات الحديثة بحيث فرق تختبر التقنيات وأخرى تكيفها لما فيه مصلحة العميل.
- تأخر العالم في انشاء المصارف الافتراضية والعملات المشفرة وهنا نجد الكثير من لجأ الى البتكوين سواء في الاستثمار او شراء احتياجاته وهذه سوق بدون رقيب والكثير من سقطو ضحايا لهذا التلاعب.

رابعا: من هم المخربون

لم يعد المخربون يجازفون بأنفسهم في تنفيذ الهجمات السيبرانية وانما قاموا بابتكار أساليب فعالة تغنيهم عن المواجهة المباشرة مع أهدافهم سواء كانت دول كما في الإرهاب السيبراني او الإرهاب المؤسسي والذي يطال مؤسسات بعينها او حتى اشخاص لعدة أسباب من أهمها:

- تطور برامج امن المعلومات والتي تسعى دائما الى اغلاق الثغرات والابلاغ عنها
- سهولة تعقب أجهزة المخربين من قبل أجهزة الامن وبالتالي الإيقاع بهم.
- الملاحقة الدولية بالتعاون المعلوماتي لما تشكله هذه الجريمة من خسائر فادحة للاقتصاد العالمي
- تطور وسائل التحريات الالكترونية وأساليب تحليل المعلومات
- تعاون شركات التواصل الاجتماعي مع الحكومات في تقديم الأدلة حول المتورطين

حتى نحدد فئة المخربين فهم ليسوا فئة واحدة كما يظن الشخص العادي وانما هناك اشخاص متعاونين معهم او حتى غافلين قد يقعوا تحت المسائلة القانونية الدولية نتيجة اهمالهم في تأمين اجهزتهم الشخصية او هواتفهم او حتى مقتنياتهم والتي تقد تلعب دور بار وتساهم في تنفيذ الهجمات بدون علم وإرادة مالكي هذه الأجهزة ومن هؤلاء الأشخاص[310]:

- **المخترقين** :هو افراد اصليين تابعين للوكالة ويقومون بعمليات اختراق الانظمة المحددة ويعملون تحت امرة القيادة ويتقاضون رواتبهم مباشرة من الجهة التي يعملون بها.
- **المأجورين** :هم من القراصنة الذي يعملون نظير مقابل مادي ولا يملكون اي اهداف خاصة ويمكن التواصل معهم عن طريق الدارك نت
- **المتعاطفين** :هم من المتعاطفون سياسيا وايدلوجيا مع قضية معينة ويعملون بدون اجر وانما نكاية بالطرف الاخر.

---

[310] روان بنت عطية الله الصحفي، مرجع سبق ذكره ص 14

- **المجربين** :هم من المبتدؤون بعالم الاختراق ويرغبون بتجربة ما تعلموه عن طريق الاخرين او من صفحات الانترنت المنتشرة.
- **الغافلين** : هم من وقعوا ضحية الاصطياد في وقت سابق وتم تثبيت برنامج خبيث بالجهاز الذي يملكونه وهو يعمل تحت تصرف المخترقين الاصلين.

خامسا بعض الاساليب وفرتها التقنيات الالكترونية العالمية المنتشرة سهلت للجماعات المخربة في التحضير او تنفيذ عمليات الارهاب السيبراني:

1) احتواء بعض التطبيقات العالمية والتي يتطلب توفرها بكل جهاز الكتروني من ثغرات امنية تم رصدها بواسطة المخربين ساهمت بشكل كبير من تنفيذ بعض الهجمات على مستوى كبير مثل الون كراي 2017[311].
2) انتشار العاب القتل الافتراضي وتسلل الجماعات المخربة والوصول الى شريحة الشباب فهي تمثل ساحات للتدريب على فنون القتال ومحاكاة لجميع العمليات التي تنوي الجماعات تنفيذها[312].
3) احتواء جميع تطبيقات التواصل الاجتماعي على خاصية النقل المباشر بدون ضوابط كافية لبث جرائم عنف وقتل او جرائم أخلاقية.
4) سهولة الحصول على حساب الكتروني بشكل سريع مما يشكل عبء كبير على أجهزة الامن في ملاحقة المجرمين.
5) سهولة الحصول على البيانات من التطبيقات العالمية وتحليلها واستهداف الاشخاص بواسطة علوم اجتماعية حديثة كالهندسة الاجتماعية في التجنيد وتأليب الافراد ضد الحكومات وتنفيذ الاجندات الخاصة بهم.
6) استمرار بعض التطبيقات العالمية مثل فيسبوك في العمل مع وجود احكام قضائية بالضلوع في التأثير في الراي العام عن طريق التحكم في مخرجات البحث او تعمد اشخاص معينين بالإعلانات والنشرات مثل خروج بريطانيا من الاتحاد الأوروبي او التأثير بالانتخابات الامريكية

[311] https://www.zdnet.com/

[312] **عياش فاطمة و بودفع علي، دراسة بعنوان "تأثير الإرهاب الالكتروني على الأطفال وطرق الوقاية" منه منشورة بمجلة الحقوق والحريات المجلد 09 العدد 01 سنة 2021، كلية الحقوق والعلوم السياسية بجامعة سكيكدة الجزائر، ص138**

7) استمرار وجود طبقات من الانترنت مثل الانترنت المظلم بالعمل بعيد عن نظر أجهزة الامن والرقابة العالمية

8) دعم بعض الحكومات للعملات الرقمية والتي ليس لها أي أسس قانونية او غطاء مقابل وعدم وجود بدائل لتحل محلها

9) التحيز من بعض وسائل التواصل الاجتماعي في القضايا الحساسة مثل تويتر والقضية الفلسطينية.

سادسا التوصيات:

1- احكام عمل التطبيقات الالكترونية والعمل على اختبارات الأمان من طرف ثالث معتمد من جهات دولية

2- وضع ضوابط أكثر لبيع واستخدام الألعاب الالكترونية

3- تحييد خاصية البث المباشر لبعض الحسابات الموثقة والمعتمدة والقديمة ومنع الحسابات الجديدة من أي نشاطات قد تشكل خطر.

4- استخدام بطاقات تعريف الهوية في فتح الحسابات الالكترونية مهما كان الهدف منها.

5- إيجاد منظومة عالمية للاحتفاظ بالبيانات وسهولة التخلص منها من قبل الافراد لمنع استغلالها مثل GDPR الأوروبي

6- تطبيق احكام أكثر صرامة في تجاوزات تطبيقات التواصل الاجتماعي وعدم الاكتفاء بالغرامة مهما كان حجمها مثل تحديد عدد المستخدمين ومنع الوصول للتطبيق من بعض الدول وغيرها

7- تنمية مهارات مأموري الضبط القضائي للوصول لخبايا الانترنت ومتابعة ما يدور فيه من تجاوزات بحق الإنسانية والقانون

8- التسريع بإيجاد بدائل محلية وإقليمية للعملات الرقمية تحت تصرف وتحكم جهات منظمة لها.

9- تعديل شروط اتاحة أي برنامج من برامج التواصل الاجتماعي عدم التحيز لاي جهة او فئة، والاكتفاء بإدارة البرنامج فقط

المراجع

1- عنترة بن مرزوق، محي الدين حرشاوي, الامن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، جامعة القاصدي مرباح الجزائر، https://www.univ-ouargla.dz/index.php

2- روان بنت عطية الله الصحفي دراسة منشورة بعنوان الجرائم السيبرانية منشورة بالمجلة الالكترونية الشاملة متعددة التخصصات، العدد الرابع والعشرون لشهر 5 2020، عمان، الأردن 2020، ص17-ص21

3- عياش فاطمة و بودفع علي، دراسة بعنوان "تأثير الإرهاب الالكتروني على الأطفال وطرق الوقاية" منه منشورة بمجلة الحقوق والحريات المجلد 09 العدد 01 سنة 2021، كلية الحقوق والعلوم السياسية بجامعة سكيكدة الجزائر، ص138

4- فاطمة عبدالله الدربي, مقالة بعنوان ما هو الامن السيبراني منشورة بجريدة البيان الاماراتية بتاريخ 13 يناير 2021، https://www.albayan.ae/opinions/by-the-way/2021-01-13-1.4064590

5- موقع https://bitcoin.org/ar/ البتكوين الرسمي تاريخ الزيارة 2021/07/22

6- موقع https://www.internetlivestats.com/ يختص بتقديم احصائيات لحظية عن الانترنت حول العالم.

7- Michael Chertoff (2017) A public policy perspective of the Dark Web, Journal of Cyber Policy, 2:1, 26-38

8- Cybercrime Laws of the United States, https://www.oas.org/juridico/spanish/us_cyb_laws.pdf

9- https://www.zdnet.com/article/leaked-nsa-hacking-exploit-used-in-wannacry-ransomware-is-now-powering-trojan-malware/

10- Bright Planet, Deep Web: A Primer, http://www.brightplanet.com/deep-web-university-2/deep-web-a-primer/.

الجلسة العلمية السادسة

رئيس الجلسة

الدكتورة الهام العلمي

أستاذة التعليم العالي، كلية العلوم القانونية والاقتصادية والاجتماعية - جامعة القاضي عياض مراكش.

الأمن السيبراني ودوره في حماية أنظمة الدفع الالكتروني

الدكتور رواد صقر

خبير التجارة الالكترونية، عضو هيئة الرقابة الإدارية ليبيا

البريد الالكتروني: rawadsagar2013@gmail.com

مقدمة:

تتخذ أنظمة الدفع الإلكترونية عدة أشكال (البطاقات الائتمانية والنقود الإلكترونية والأوراق التجارية الإلكترونية) كلها تعتمد اعتماداً كلياً على معاملات المؤسسات المالية والبنكية التي تتم عبر الإنترنت.

فلقد تنوعت أعمال البنوك وتغيرت طرق تقديمها لخدماتها، فتولدت فئة جديدة من العملاء تطلبت عملية تداول ذات طاقات استيعابية تتناسب مع الأحجام الكبيرة للمدفوعات بين الشركات وتحقق البيع المباشر للمستهلك عبر الإنترنت، وتولدت بالتالي فرص للتعامل المباشر بين المستهلك والشركات، وبدأت هموم هذه الشركات تتوجه إلى عمليات مالية أكثر تفاعله مع الشبكة والمشاركة في التطورات المستقبلية في إدارة النقد بواسطة البرمجيات، وفي نفس الوقت احتاجت هذه البرمجيات إلى ضمانات عالية جداً من الأمن في تبادل الملفات البنكية عبر الشبكة، خشية العبث بها أثناء عملية المرور من بنك لآخر، ونظراً لعدم توفر هذه الضمانات لجأت أغلب البنوك إلى تكنولوجيا التشفير، لكل ذلك يتم اللجوء لوسائل أمان فنية لتوفير الثقة بين المتعاملين وضمان فعالية تلك الوسيلة في الوفاء لتيسير وازدهار التجارة الإلكترونية ولتضمن الوفاء والدفع السريع والآمان خلالها.

وتتولى الجهة التي تقدم خدمة الوفاء الإلكتروني هذه المهمة، حيث يتم تحديد الدائن والمدين أطراف العملية التي تتم بطريقة مشفرة من خلال برنامج معد لهذا الغرض، بحيث لا يظهر الرقم البنكي على الشبكة، ويتم عمل أرشيف يسهل الرجوع إليه للمبالغ التي يتم السحب عليها بهذه البطاقة، وهذا ما يطلق عليه نظام المعاملات الإلكترونية الآمنة (Set)، باعتبار أن هذا النظام يحقق عدة ضمانات أساسية أهمها التكاملية، أي ضمان أن الرسالة المرسلة هي الرسالة المستقبلة عن طريق البصمة الرقمية وسرية المعاملة من خلال تشفير

محتوى الرسالة والتحقق من شخصية صاحب بطاقة الائتمان البنكية وشخصية البائع، حيث يقوم البنك باتخاذ الإجراءات المالية وإخطار الطرفين بإتمام المعاملات.

وبالتالي يبقى استعمال أنظمة الدفع الإلكترونية مرهون بتوفير قدر من الحماية التقنية التي يضمنها المتعاملون بها؛ كمقدمي الخدمات على الخط والبنوك في مجال استعمال التكنولوجيا الحديثة للاتصالات التي تعتمد أساساً على برامج الحواسيب وقواعد البيانات المشفرة لحمايتها من الاختراق والسرقة[313]، فالغوص في العالم الافتراضي للدفع الإلكتروني الذي يتبلور من خلال شبكة الانترنت سيؤدي إلى التعرض لبعض الإشكالات التي منها عدم الاستقرار في التعاملات نتيجة لعدم إمكانية توفير الأمن الذي يؤدي بدوره إلى عدم الثقة في استخدام أنظمة الدفع الإلكترونية، مما استوجب معه ضرورة العمل على إيجاد وسائل وتقنيات وضعت تحت تصرف المتعاملين بها كي تضمن قدر ممكن من الثقة والاطمئنان لمستعملي هذه الأنظمة والتي يطلق عليها مصطلح الامن السبيري.

ومن هذا المنطلق جرى التركيز والتشدد عند إنشاء أنظمة الدفع الإلكترونية على سياسات وإجراءات الحماية الواجب اتباعها في تصميم النظم والبرمجيات التي تقدم هذه الخدمات، وكذلك في متابعة ومراقبة حسن تنفيذها من قبل المتعاملين بها، إضافة إلى الإجراءات الوقائية الواجب اتخاذها، وذلك للتخفيف من الأذى القابل الحدوث في حال اختراق هذه الأنظمة من قبل بعض الجهات العابثة بهدف مقصود أو بسوء نية، في الوقت الذي تعتبر فيه المؤسسات المالية والمصرفية المصدرة لأنظمة الدفع هاته من المؤسسات الاقتصادية الهامة في أي دولة من دول العالم، لعل هذا ما جعل معه الحاجة ملحة إلى ضرورة اتخاذ العديد من الإجراءات المشددة من الحيطة والحذر والحماية والمراقبة عند تقديم هذه المؤسسات خدماتها الكترونياً.

وتماشيا مع التطور الهائل الذي شمل قطاع تقنية المعلومات على مختلف الأصعدة وانفجار ثورة التكنولوجيا المصرفية والتي حققت نتائج إيجابية من اختصار الوقت والجهد وتأمين سرعة التعامل بأنظمة الدفع الإلكتروني،

---

[313] إن حماية قواعد البيانات من الاختراق والسرقة تعتبر من أكثر المسائل أهمية وأولوية بالنسبة للمبرمج الإلكتروني، ويوجد هناك وجهان رئيسيان لحماية قواعد البيانات، الأول يتعلق بحقوق المبرمج المتمثلة في حقوقه الفكرية، والثاني يتعلق بالعملاء المستخدمين للبرامج وكيفية منح الصلاحيات للمستخدمين. راجع: أمجد جمالي، حماية قواعد البيانات وصلاحيات المستخدمين، مقال منشور على الرابط الالكتروني التالي: مجلة الفريق العربي، 2 أبريل 2002، ص 1.

-www.arabteam2000.farum.com.

فإنه يجب توفير الضمان والثقة اللازمين لإنجاح استعمال هذه الأنظمة من جهة، واعتماد الكثير من التقنيات لتأمين حماية معاملات الدفع الإلكتروني من جهة أخرى.

ولتوفير الأمن يجب استخدام أحد الوسائل التي تم إيجادها للوصول لاستقرار في التعاملات المالية الإلكترونية ومن هذه الوسائل نهج بعض البرامج الآمنة للمعاملات المالية والتي يطلق عليها اسم البرتوكولات المؤمنة (المبحث الأول)، وإذا كانت مهمة حماية أنظمة الدفع الإلكترونية تقع على أصحاب الاختصاص والتقنيين لمعرفتهم بتلك المهارة وكيفية ردع الاعتداءات بمناسبة استعمال البيانات الإلكترونية وانتقالها، فإن هذه الحماية لا تكفي وحدها إذا لم تكن مدعمة بحماية قانونية تتمثل في سن مجموعة من النصوص التي تنظم وتحكم معاملات الدفع الالكتروني، التي تتطلب بدورها تكثيفاً للجهود على المستويين الداخلي والخارجي واتباع إجراءات المصادقة الإلكترونية (المبحث الثاني)

المبحث الأول: بروتوكولات الامن السيبراني

تستخدم البروتوكولات في مجالات الاتصالات بين الحواسيب، ويقصد بها مجموعة القواعد والأسس التي تحدد طريقة إرسال البيانات وانتقالها عبر خطوط الاتصالات من جهاز حاسوب لآخر وكيفية استقبال هذه البيانات عندما تصل إلى محطتها الأخيرة[314]، فالبروتوكول بهذا المعنى هو مجموعة من القوانين التي تحدد وتفصل كيف لحاسبات آلية أن تتصلا ببعضها البعض عبر شبكة ما. ومن أهم خصائص بروتوكولات الإنترنت أنها قادرة على العمل على عدة محاور أي أن النظام يدعم برمجيات وحواسب آلية مصنعة من شركات مختلفة وهذا (بالنسبة أنظمة الدفع الإلكترونية)

يعني بأن الزبائن وأصحاب العمل لن يضطروا أن يشتروا أنظمة معينة من أجل تسيير التجارة، أضف إلى ذلك أن جميع البروتوكولات تعمل في طبقات، بحيث أن كل طبقة تبدأ عملها بعد أن تنتهي الطبقة التي تحتها أو فوقها وكل طبقة تستخدم البيانات الناتجة من الطبقة التي فوقها أو تحتها وكل طبقة في البناء مسؤولة عن بعض من العمليات والمهام، إضافة إلى أنها قادرة على تفسير وقراءة البيانات التي تحدث فقط في طبقة التطبيق وليس في طبقات الشبكة، وتتعدد البروتوكولات وتتنوع من أجل تسهيل انتقال البيانات والمعلومات بين المحطات الإلكترونية، وتحمل مستويات متعددة، رغم أن البروتوكولات الداعمة للعملية الأساسية لشبكة

[314] طارق عبد العال حماد، التجارة الإلكترونية، بدون ذكر الطبعة، الدار الجامعية للنشر والتوزيع، الإسكندرية/مصر، 2005، ص 732-736.

الانترنت هما (IP-TCP) [315] بروتوكول مراقبة البث أو الحكم بالإرسال وبروتوكول الانترنت، ويشملان قواعد أساسية حول كيفية نقل البيانات عبر الشبكة وكسرها، ويقدمان حلولا في مجال الاتصال ما بين الشبكات العالمية.

فبروتوكول (TCP) يراقب تجميع الرسالة في رزم متماثلة قبل بثها على الشبكة العنكبوتية كما يراقب إعادة تجميع رزم حتى تصل إلى وجهتها بعد أن يتأكد بأن الحاسبين الآليين يستطيعان الاتصال ببعضهما البعض بطريقة يعول عليها، وكل اتصال لبروتوكول التحكم بالإرسال يجب أن يقابله أشعار باستلام البيانات فإذا لم يتم الحصول على هذا الأشعار بعد فترة معينة فإن الجهاز المرسل يقوم بإعادة إرسال البيانات، ولكي تتم عملية الإرسال أو عملية إجابة لطلب فإن المرسل يجب عليه تقسيم هذا الطلب إلى عدة رزم صغيرة كل رزمة تحوي عنوان الجهاز المرسل والجهاز المستقبل، وهنا يتدخل بروتوكول الانترنت لينسق الرزم ويوزع العناوين.

ويعتبر بروتوكول (IP) أحد أهم البروتوكولات الأساسية وهو عبارة عن رقم مكون من أربعة أجزاء يعرف الجزء الأول من الرقم بدءا من اليسار المنطقة الجغرافية والجزء الثاني يحدد المنظمة أو الحاسب المزود أما المجموعة الثالثة من الأرقام فتحدد مجموعة الكمبيوترات التي ينتمي إليها الجهاز والمجموعة الرابعة تحدد الجهاز المستخدم ويمكن اعتبار الـ (IP) نوع من الخرائط الخاصة بالإنترنت حيث يمكن الاتصال بأي موقع من خلال نقطة معينة على هذه الخريطة،

وتفسير ذلك أن كل مستضيف على أي شبكة يكون له رقم هوية منطقي يسمى بعنوان بروتوكول الإنترنت وهو نفسه العنوان المنطقي، وبروتوكول الإنترنت يحصل على الأجزاء من طبقة المضيف ويكسرها إلي رزم، وبروتوكول الإنترنت في الجهاز المستقبل يقوم بإعادة جمع تلك الرزم ويحولها إلى أجزاء، وكل رزمة تحوي عنوان بروتوكول الإنترنت للجهاز المرسل وللجهاز المستقبل، وعندما تصل الرزمة إلى الموجه فإنها تقوم بقراءة عنوان بروتوكول الانترنت الموجود في الرزمة ومن ثم يقوم بعملية التوجيه الصحيحة، وتضم البروتوكولات (IP-TCP) العديد من التطبيقات المتنوعة التي تقدم الخدمات للمستخدمين وأحيانا تعرف بأنها خدمات التطبيق

[315] بروتوكول (IP)Internet Protocol: يستخدم هذا البرتوكول في إيجاد عنوان لشبكات الانترنت أي أنه يتحكم ويضع القواعد لإرسال واستقبال الملفات باستخدام عناوين الانترنت الرقمية وتوفر الطبعة الأخيرة من بروتوكول الانترنت خيارات أكثر متعددة الوسائط وأمنا إضافيا وعناوين أكثر لأجهزة الشبكة.

- بروتوكول Transmission contralprotocol: يستخدم هذا البروتوكول في تبادل الرسائل بين مواقع الانترنت المختلفة على مستوى أجزاء الملفات الصغيرة والتي يطلق عليها الحزم « Packets ».

وهي تشمل عرض صفحة الويب وتسهيلات إدارة الشبكة ونسخ الملفات والبريد الإلكتروني وخدمات الدليل[316].

وأمام وسائل الاختراق التي يقوم بها قراصنة الشبكة العنكبوتية التي تحاول التركيز على معرفة رقم بروتوكول الانترنت الخاص بالمستخدم، قام العديد من مؤيدي تطوير التجارة الإلكترونية عموماً والدفع الإلكتروني على وجه الخصوص إلى وضع العديد من برامج أمن المراسلات عند استخدام أنظمة الدفع الإلكترونية وذلك بهدف ضمان الثقة في هذه المعاملات مما يساعد على تطويرها وترقيتها، والتي تسمى اصطلاحاً بالبروتوكولات.

المطلب الأول: بروتوكولات تأمين البيانات المالية

تشمل بروتوكولات تأمين البيانات المالية كل من بروتوكول الطبقات الآمنة وبرتوكول الحركات المالية الآمنة، ويعتبران من أهم بروتوكولات أمن المعاملات الإلكترونية لتحقيقها غاية ضمان الحفاظ على أمن البيانات (خصوصيتها وسلامتها والتحقق من وصولها إلى الجهة المطلوبة) أثناء إجراء الحركات المالية عبر شبكة مفتوحة مثل الانترنت. ويشار لبروتوكول (الحركات المالية) التحويلات الإلكترونية الآمنة اختصارا بـ (Set)[317]، وهو من تطوير شركتي فيزا وماستركارد، وذلك لتأمين انجاز التحويلات المالية بواسطة البطاقات المصرفية عبر الشبكات المفتوحة، أما بروتوكول طبقة المقاييس الآمنة (الطبقات الأمنية لتأمين) فيشار إليه اختصارا (SSL)[318]، وقد طور بمعرفة شركة نت سكيب لتأمين نقل آمن للمعلومات بين خادم الويب ومستعرضات الويب ولكي يضمن الخصوصية خلال عمليات التبادل عبر شبكة الانترنت.

الفقرة الأولى: بروتوكول الطبقات الآمنة (SSL)

هو برنامج به بروتوكول تشفير متخصص لنقل البيانات والمعلومات المشفرة بين جهازين عبر شبكة الانترنت بطريقة آمنة، بحيث لا يمكن لشخص قراءتها غير المرسل والمستقبل، وتكون قوة التشفير فيها قوية ويصعب فكها، وسمي هذا البرتوكول بالطبقة الآمنة لأن البرنامج الذي يستخدم من خلاله يعمل كطبقة وسيطة تربط بين بروتوكول التحكم بالنقل وبروتوكول (http://(hypertext.transfer.protocal) وقد طور هذا البرتوكول

---

[316] طارق طه، التسويق بالانترنت والتجارة الالكترونية، بدون ذكر الطبعة، دار الفكر الجامعي، الإسكندرية/مصر، 2006، ص 61.

[317] (Set): Secure electronic transaction.

[318] (SSL): secure sockets dayer.

من طرف شركة نت سكيب[319]، لتأمين نقل أمن المعلومات بين خادم الويب ومستعرضات الويب، ويعتمد هذا البروتوكول على خوارزمية المفتاح العام والمفتاح الخاص، إذ يزود الخادم المستفيد بالمفاتيح العامة، وتستخدم هذه الأخيرة في تشفير الرسائل المتجهة إلى الخادم، ولا يمكن استخدام المفتاح العام لفك شيفرة الرسالة التي شفرها، إذ يتفرد المفتاح الخاص (لدى الخادم) بالقدرة على فك شيفرة الرسالة التي شفرها المفتاح العام، وبذلك فهو يختلف عن بقية طرق التشفير في شيء واحد، ألا وهو عدم الطلب من مرسل البيانات اتخاذ خطوات لتشفير المعلومات المراد حمايتها، وكل ما يفعله المستخدم هو التأكيد من استخدام هذا البروتوكول بالقوة المطلوبة، وبذلك يستطيع المستفيد بالطريقة ذاتها إنشاء زوج من المفاتيح العامة والخاصة لإرسال المعلومات إلى الخادم. وتمنع هذه الطريقة ظهور مشاكل الاتصال مثل التجسس أو التنصت عند كشف المعلومات الحساسة (مثل البيانات الشخصية أو أرقام بطاقات الائتمان ضمن أحد مواقع الويب)

ويساعد بروتوكول الطبقات الأمنية (SSL) في التحقق من المفتاح العام الذي أصدره الخادم، ويتأكد من عدم تغير المعلومات أثناء التحويل، وذلك باستخدام الشهادات الرقمية التي تصدر من تغير المعلومات أثناء التحويل والتي تعطيها الجهات المانحة[320]، الموثوق بها التي توقع عليها، وتستخدم هذه الشهادات للتحقق من موثوقية المفاتيح العامة التي أصدرت. عليه سنتناول كلاً من برنامج تشغيل الطبقات الآمنة (أولا) ثم آلية عمل هذا البرتوكول (ثانيا).

أولا: برنامج تشغيل بروتوكول الطبقات الآمنة

يقوم برنامج تشغيل بروتوكول المقاييس الآمنة بربط المتصفح الموجود على جهاز المستخدم (المشترى) بجهاز الخادم الخاص بالموقع المراد الشراء منه، ويجب أن يكون والحالة هذه الخادم مزوداً بهذه التقنية، ثم يقوم هذا البرنامج بتشفير أي معلومة صادرة من ذلك المتصفح وصولا إلى جهاز الخادم الخاص للموقع، باستخدام بروتوكول التحكم بالإرسال وبروتوكول الانترنت (TCP/IP) السابق الإشارة إليهما، إذ يزود الخادم المستفيد بالمفاتيح العامة، وتستخدم هذه المفاتيح العامة في تشفير الرسائل المتجهة إلى الخادم، ولا يمكن استخدام المفتاح العام لفك شفرة الرسالة إلى شفرها، إذ يتفرد المفتاح الخاص (لدى الخادم) بالقدرة على فك شفرة الرسالة التي شفرها المفتاح العام، ويستطيع المستفيد بالطريقة ذاتها إنشاء زوجاً من المفاتيح العامة والخاصة لإرسال المعلومات إلى الخادم.

---

[319] http://www.retscape.com.

[320] CA : certificate authorities.

وبالتالي يقوم الشخص أو المؤسسة في ظل هذا البرنامج التشغيلي للبروتوكول بتوليد زوج من المفاتيح العامة والخاصة، ثم يرسل المفتاح العام إلى الجهة مانحة للشهادة لتضيف الجهة المانحة بعض المعلومات المتعلقة بالشهادة (كالاسم ورقم التعريف، وعنوان البريد الإلكتروني، وتاريخ الانتهاء والرقم التسلسلي) وتوقيع عليها بالمفتاح العام لطالب الشهادة وبالمفتاح الخاص للجهة المانحة للشهادة، ويصادق توقيع الجهة المانحة للشهادة على المعلومات المضافة إلى الشهادة وعلى المفتاح العام الموجود ضمن الشهادة. ويمكن أن ترسل الجهة المانحة الشهادة إلى طالبها أو تنشرها للعموم، أو تحتفظ بها في خادم الشهادات كقاعدة بيانات تسمح بتسليم واسترجاع الشهادات الرقمية، وعند فك شفرة الوثيقة المصدقة رقميا، تستخدم البرمجيات من الطرف المستقبل المفتاح العام للجهة المانحة للشهادة، فإن نجحت عملية فك شيفرة الشهادة،

فإن ذلك يعني أن الجهة المانحة التي وقعت الوثيقة هي التي أنشأتها بالفعل، وتستطيع البرمجيات من الطرف المستقبل فحص جميع معلومات الشهادة المتعلقة بمالكها، مما يمكن المستقبل من الحصول على المفتاح العام للمالك (من الشهادة) للتحقق من توقيع المرسل، فإن تمكن هذا المفتاح العام المصدق من فك شفرة توقيع المرسل، يصبح المستقبل على ثقة بأن التوقيع أنشئ باستخدام المفتاح الخاص للمالك[321].

ثانيا: آلية عمل بروتوكول الطبقات الأمنية

ينشئ المستفيد المشتري (زائر الموقع) اتصالا بخادم آمن، ويميز الخادم الآمن بإلحاق حرف "د" بنهاية اسم البروتوكول ضمن عنوان محدد المصدر URL (مثلا http://server.com)، وبعد إنشاء الاتصال، يبدأ المستفيد جلسة المصافحة وذلك بإرسال رسالة أو عبارة ترحيب تستفسر عن هوية الخادم وتخيره بقدرات التشفير لدى المستفيد، ويرد الخادم برسالة أو عبارة ترحيب، وإرسال شهادته الرقمية وبعض قوائم خوارزميات التشفير، ويقوم المستفيد بفحص الشهادة الرقمية للخادم كأن يبحث عن مصدرها وتاريخ انتهائها،

وكذلك تتم المقارنة بين اسم الموقع على الشهادة مع اسم الموقع في جهاز الخادم والمقارنة بين الرقم العام المرسل من الجهاز الخادم إلى المتصفح مع التوقيع الإلكتروني للمؤسسة، وذلك للتحقق من أنها قد صدرت عن جهة مانحة معتمدة، وبعد تحقق كل طرف من الطرف الآخر، يتفق الخادم والمستفيد على معيار التشفير الذي يستخدم في جلسة تبادل البيانات وفقا لبروتوكول الطبقات الأمنية.

---

[321] عبد الرحمان بن ناصر العمري، الإنترنت ودورها في التجارة الإلكترونية، المرجع السابق، ص55.

وبعد الانتهاء من جلسة المصافحة في بروتوكول الطبقات الأمنية، يولد المستفيد مفتاحا سريا للجلسة، ويشفره باستخدام المفتاح العام للخادم، ثم يفك الخادم شفرة مفتاح الجلسة باستخدام مفتاحه الخاص، ويستخدم كل من الخادم والمستفيد هذا المفتاح الفريد لتبادل المعلومات الحساسة في جلسة بروتوكول الطبقات الأمنية ولا يصلح هذا المفتاح الفريد إلا لجلسة واحدة، وكل هذه الخطوات تتم للتأكيد من مصداقية الموقع وحماية المستهلكين من المؤسسات الوهمية، علما بأن جميع هذه الخطوات تتم بواسطة المتصفح لدى الزبون دون علمه أو تدخله، وفي حالة عدم المطابقة أو الالتباس أو إذا كانت هناك ملاحظات، يقوم المتصفح بإعلامه بالنتيجة.

الفقرة الثانية: بروتوكول الحركات المالية الآمنة (SET)

طورت مجموعة من الشركات العالمية الرائدة كمايكروسوفت (Microsoft) وآي بي إم (IBM) ونتسكيب (Netscape) وفيزا (VISA) وماستركارد (Master card)[322] بروتوكولاً لعمليات الدفع أطلقت عليه اسم بروتوكول الحركات المالية الآمنة (SET)، والغاية من هذا البروتوكول ضمان الحفاظ على أمن البيانات أثناء إجراء الحركات المالية عبر شبكة الانترنت، ويشبه هذا البروتوكول، بروتوكول الطبقات الآمنة (SSL) في استناده إلى التشفير والتوقيعات الرقمية، وللحفاظ على خصوصية وسلامة المعلومات المنقولة عبر الانترنت بين حاملي البطاقات والتجار، ويختلف معه في كونه (SET) برمجيات تدعى برمجيات المحفظة الإلكترونية تحتوي على رقم حامل البطاقة والشهادة الرقمية التابعة له، يضاف إليها في حالة التاجر شهادة رقمية صادرة عن أحد البنوك المعتمدة ويستخدم كل من حامل البطاقة والتاجر الشهادة الرقمية التابعة له، مما يتيح لكل منهما التحقق من هوية الآخر عند إجراء الحركات المالية عبر الانترنت[323]، ولا يمكن للتاجر مشاهدة رقم البطاقة الائتمانية أثناء جلسة بروتوكول الحركات المالية الآمنة حيث ترسل الصيغة المشفرة لهذا الرقم إلى مصدر هذه البطاقة للموافقة على إجراء الحركة المالية مع التاجر وتضمن هذه الطريقة عدم عرض الرقم كما تمنع أي تعديل غير مرخص به أثناء إرسال البيانات[324].

---

[322] لقد تم التعاون بين أكبر مؤسسات لإصدار بطاقات البنكية في العالم وهو مؤسسة الفيزا وماستركارد، وانضمت إليها أمريكان إكسبرس: وذلك في عام 1996 لإصدار نظام جديد مشترك للمعاملات الالكترونية الآمنة وهو برتوكول الحركات المالية الآمنة (SET) secureelectronic transactions .

[323] منير الجنيهي وآخرون، البنوك الإلكترونية، بدون ذكر الطبعة، دار الفكر الجامعي، الإسكندرية/مصر، 2006، ص 41.

[324] نادر شبعان إبراهيم السواج، النقود البلاستيكية وأثر المعاملات الالكترونية على المراجعة الداخلية في البنوك التجارية، بدون ذكر الطبعة، الدار الجامعية، مكان النشر مجهول، 2006، ص 124.

المطلب الثاني: نظم تأمين وحماية الحسابات المالية

بهدف تطوير الدفع الإلكتروني قامت مؤسسة فيزا كرد بتطوير نظام يسمى بـ (3Ds) لأجل تعزيز عمليات الوفاء بواسطة البطاقات الائتمانية، فهذا النظام يوفر أعلى مستويات الحماية لعمليات الدفع عبر الانترنت، حيث يساهم في تخفيض نسبة الأخطار أو المشاكل التي تحدث خلال عملية الشراء عبر الانترنت من خلال تمكين البنوك المتخصصة في إصدار البطاقات والتحقق من هوية الشخص الذي قام بإجراء المعاملة التجارية الإلكترونية، وتوفر تقنية (3 دي أس) حماية إضافية حيث تتم العمليات الإلكترونية أمام الشخص مباشرة، كما يعتمد على نظام التشفير (SSL) لتمرير المعلومات والتأكد من هوية حامل البطاقة خلال عمليات الشراء التي تتم على الخط، ويجمع هذا النظام بين السهولة ومرونة التطبيق، ويوفر الانتقال الآمن لتفاصيل الحساب وتخفيض نسبة الأخطاء[325].

أما فيما يتعلق بعالم الحسابات المركزية الكبيرة لا يوجد الكثير من نظم التي توفر الأمن فيها، وربما السبب هو سيطرة بعض الشركات الكبرى على سوق الحسابات المركزية، وتتميز هذه السوق بضخامة الإنتاج حيث يجب أن تكون نظم الأمن فيها شاملة ومتناغمة مع نظام التشغيل الرئيسي ومع العديد من نظم التشغيل المساعدة ولذلك تحجم شركات نظم أمن المعلومات الصغيرة على الدخول إلى هذه الأسواق وتنفرد به شركات مثل (IBM) لذلك نجد على رأس نظم أمن الحسابات المركزية الشهيرة نظامين هما نظام "راكف-RHSC"[326] ونظام "ACF"[327]. وإلى جانب تقنية (3Ds)، ونظام أمن الحسابات المركزية، يوجد نظام آخر يسمى بنظام أمن الحسابات الشخصية وهو الذي يهمنا هنا، الذي يحتوي على العديد من البرامج كبرنامج بي سي سيف (PC

---

(325) Steven J. Murdoch t Ross Anderson, Vérifiré par et Master carde Secure code, étude du laborative informatique, université de Cambridge. Royaume uni, in : http://www.cl.com.uk/users/.p.2. Voir aussi : tout système de paiement électronique sur internet passe par emploi du protocole SSL (Secure socket layer) qui chiffre les données pour que SSL fonctionne, un certificat (document électronique qui certifie sui vous êtes) est émis par une autorité de certificat, c'est une organisation dont le rôle consiste à prouvé l'identité des entreprises. Voir : Brenda Kieman, -commerce stratégie a solutions, Microsoft presse, Paris, 2001, p. 250. Il est important pour le commerçant d'y joindre un système de vérification d'adresse. Malgré tout, les petites et moyenne entreprises ont l'avantage a utiliser SSL qui leur offre un mécanisme de paiement efficace. Voir aussi : Pierre- Paul Lemyre, Le guide juridique du commerçant électronique, in : www.juristint.org.

(326) RACF: Ressource Access ContralFacility.

(327)ACF: Access control facility.

وهي أنظمة تتميز بمحدودية الاستعمال فهي أنظمة قليلة الانتشار بضرورة توافقها مع أنظمة منتجيها كشركة IBM. انظر محمد دباس الحميد، ماركو إبراهيم نينو، حماية أنظمة المعلومات، ط ا، دار الحامد للنشر والتوزيع، عمان/ الأردن، 2007، ص 105-106.

safe) وبرنامج إيزاك 2200 (ISCA 2200)، إضافة إلى برنامج ديسك ووتشر (Watchr Disk) وبرنامج ميل سيف (Mail Safe) التي سنتناولها في (الفقرة الأولى) ونخصص الفقرة الثانية لوسائل التأمين عن طريق التحكم في عملية الدخول أو الخروج (الفقرة الثانية).

الفقرة الأولى: نماذج لبعض برنامج تأمين الحسابات البنكية

أولا: برنامج بي سي سيف (PC. Safe)

يعتبر برنامج (بي سي سيف) أسلوبا للتحكم في استخدام البيانات، فهو يستخدم كلمة مرور لمرة واحدة لتنظيم استخدام الحاسب، ويعتبر هذا البرنامج من انتاج شركة "اينجما لوجيك" إذ أحدثوا من خلاله كلمة مرور تستخدم لمرة واحدة، ولا يشترط أن يكون ذلك من خلال نظام التشغيل الذي تم من خلاله تشفير البيانات بل من خلال أي نظام تشغيل آخر، ويتطلب ذلك وسائل خاصة تتيح استخدام كلمة المرور التي تستعمل فقط لمرة واحدة[328]. كما يسمح برنامج (PC- Safe) بتشفير البيانات بواسطة المستخدم والاحتفاظ به في الصورة المشفرة ولا يمنع ذلك من استخدامه من قبل مستخدمين آخرين بافتراض أنهم مصرح لهم بذلك، فعند طلبها من المستخدم الجديد يتم تشفير إجراء البيانات التي يحتاج إليها. فيقاوم هذا البرنامج محاولة اكتشاف كلمة المرور عن طريق التجربة والخطأ؛ لأنه يتوقع كلمة مرور مختلفة في كل مرة، وبذلك فإذا تمكن أحد المستخدمين من اكتشاف كلمة المرور الخاصة بمستخدم أخر لن تنفعه إذا أراد الدخول بها بعد خروج المستخدم الحقيقي؛ لأن في هذه الحالة سيتوقع كلمة مرور جديدة، وهذا يدل على أن برنامج (PC. Safe) ذات أهمية كبرى كونه نظيراً للأمن الإعتيادي[329] الذي يتم فيه استعمال البطاقة الذكية (Smart card) الخاصة بالمستهلك، فعندما يقوم هذا الأخير بعملية الشراء يدخل بطاقته بقارئ خاص يسمى (Pin pad) ثم يكتب عليه مبلغ الشراء ورمزه السري، وتتم عملية التأكد من الرمز محليا، أي أن الرمز السري يترجم مباشرة من قبل القارئ ولا يرسل عبر الشبكة لتتم مراقبته عن بعد[330]،

---

[328] واقد يوسف، النظام القانوني للدفع الإلكتروني، المرجع السابق، ص 168.

[329] Sécurité Hardware, Reboul P Xardel D, 1997, p. 145.

[330] لعل من أهم المزايا التي يوفرها هذا الحل الأمني: قراءة الرمز محليا، والوقاية من أي عملية قرصنة، صعوبة نسخ البطاقة الذكية، أو أن ينسخ رقمها، والرمز السري لا يعرفه إلا حاملها الذي يمكن التعرف عليه بإجراءات أمنية بسيطة، بحيث أصبحت عملية إدخال وإفراج البطاقة سهلة بالمقارنة مع تحويل برنامج التشفير إلى الحاسب ومنه أصبح استعمال وسيلة الدفع بصفة مستقلة عن الحاسب النهائي، كما تعتبر البطاقة الذكية وسيلة اعتيادية لا تتطلب تعليم معقد للمستعمل؛ يعتبر تقديم الرمز السري أثناء قراءة البطاقة بمثابة إمضاء الكتروني وتصبح إرادة الشراء غير مشكوك فيها وإمكانية نقض المعاملة مستحيلة.

ولعل هذا ما جعله يصبح في الوقت الراهن أحد أهم البرامج المجهزة داخل الحاسب الآلي المزود بقارئ البطاقات المصرفية، التي تعتبر أكثر فعالية من حيث الأمن في المعاملات، التي جعلت البطاقات الذكية تغزو العالم تدريجيا بفضل مشروع البطاقات الذكية الدولية[331].

ثانيا: برنامج إيزاك 2200 (ISAC 2200)

يقوم برنامج ايزاك 2200 بتصنيف المستخدمين الذين يحق لهم استخدام كل برنامج ويفتح حق الاستخدام للمستخدمين الذين تنطبق عليهم شروط الصلاحية المحددة بالسجل، فهو يفرض استخدام مواصفات قياسية خاصة حتى يحتفظ بسجل لكل ملف، ويعتبر هذا البرنامج من إنتاج إيزولشن سيستمز (Isolation systems) الكندية الذي يعد وهو امتداداً لنظام التشغيل Dos[332].

وفي هذا الإطار ولكي يتم حفظ سلامة المعلومات ذات القيمة المالية، يجب حماية عمليتي نقل هذه المعلومات وتخزينها، وذلك لمنع أي تغيير للمحتوى بشكل معتمد، بشكل يؤدي إلى الحفاظ على محتوى مفيد وموثوق به، وفي الغالب تكون الأخطاء البشرية وعمليات العبث المقصودة هي السبب في تلف أو تشويه البيانات، ولتفادي ذلك (تشويه أو تلف البيانات) يمكن استخدام تقنيات مثل البصمة الالكترونية للرسالة واستحضار تقنية التشفير، ومن المفيد استخدام برمجيات مضادة للفيروسات لحماية التخزين من انتهاكات الفيروسات التي تتسبب في تلف أو تشويه البيانات، ومن المهم أيضا الاحتفاظ بنسخ احتياطية لاسترداد البيانات المفقودة في حال تعرضها للضرر، أو في حالة تعطل الشبكة أثناء عملية النقل.

ثالثا: برنامج ديسك ووتشر وبرنامج ميل سيف

يعتبر برنامج ديسك ووتشر (Watcher Disk) هو احد من المجموعة التي صممت لحماية البيانات ولضمان عدم محوها عن طريق خطأ غير مقصود من جانب المستخدم[333]، على عكس برنامج ميل سيف (Mail Safe) الذي تم وضعه من طرف شركة (RSA Security Data)، ويعتمد هذا البرنامج على تشفير الملفات من أجل تأمين الاتصالات وحالات التشارك في البيانات وهو أكبر البرامج انتشارا ونفعا وجاذبية في حالات البريد الالكتروني كونه يتيح ما نطلق عليه بالأغلفة الرقمية والتوقيعات الرقمية، فبينما تخفي الأغلفة الرقمية

---

(331) يحمل مشروع البطاقات الذكية الدولية رمز EMV (Eurocard. Master card Visa)

(332) واقد يوسف، النظام القانوني للدفع الإلكتروني، المرجع السابق، ص 269.

(333) برنامج Watcher Disk يقوم على سبيل المثال باستبدال الأمر format ويصبح مكانه أمر آخر يتطلب تأكيداً من المستخدم عند استخدامه، انظر: محمد دباس الحميد، ماركو إبراهيم نينو، حماية أنظمة المعلومات، مرجع سابق، ص 108.

المعلومات عن الجميع ما عدا الجهة المقصود وصول الرسالة إليها، نجد أن التوقيعات الرقمية تنسب الرسالة إلى مرسلها الحقيقي وتمنع من إحداث أي تغيرات من غير المرخص بها الرسالة[334].

الفقرة الثانية: التأمين عن طريق التحكم في عملية الدخول والخروج

إضافة إلى جميع البروتوكولات والأنظمة الخاصة بالتأمين والحماية التي تم استعراضها سلفا توجد بعض الأنظمة التأمينية الأخرى التي تتحكم في عمليات دخول وخروج البيانات أو الأشخاص، ومن أهم تلك الأساليب التأمينية وأشهرها، اسم المستخدم وكلمة السر والبصمة الإلكترونية (أولا) والخادم المفوض أو الموكل (ثانيا).

أولا: اسم المستخدم وكلمة السر والبصمة الالكترونية

تساعد هذه الطريقة التأمينية في عملية التحكم في إمكانية دخول بعض الأشخاص على أنظمة معينة أو على شبكات معينة أو حتى اطلاعهم على مواقع معينة أو بيانات تشتمل عليها تلك المواقع ويتم ذلك عن طريق حمل الشخص المسموح له بالدخول على النظام أو الاطلاع على البيانات لاسم خاص به لاستخدامه في عملية الدخول، وكذلك كلمة سر معينة لا يعرفها سواه أو رقم سري[335].

ورغم أن التشفير يمنع المتخصصين من الاطلاع على محتويات الرسالة إلا أنه لا يمنع المخربين من العبث بها، أي أن التشفير لا يضمن سلامة البيانات، ومن هنا ظهرت الحاجة إلى البصمة الالكترونية للبيانات، وهي بصمة رقمية يتم اشتقاقها وفقا لخوارزميات معينة، تدعي (دوال أو اقترانات التقوية) إذ تطبق هذه الخوارزميات حسابات رياضية على الرسالة لتوليد بصمة تمثل ملفاً كاملاً أو رسالة وتدعى البيانات الناتجة بالبصمة الالكترونية للبيانات التي تتكون من بيانات لها طول ثابت يتراوح ما بين 128 و160 بث وتؤخذ من الرسالة المحولة ذات الطول المتغير، وتستطيع هذه البصمة تمييز الرسالة الأصلية (البيانات) والتعرف عليها بدقة، حتى إن أي تغيير في الرسالة ولو كان "بث" واحداً سيفضي إلى بصمة مختلفة تماما. كما تتميز البصمات الإلكترونية (التي لا يمكن اشتقاقها دائماً من رسالتين مختلفتين) عن بعضها البعض بحسب المفاتيح الخاصة

---

[334] واقد يوسف، النظام القانوني للدفع الإلكتروني، مرجع سابق، ص 169.

[335] عبد الرزاق نصر العجيلي، التجارة الإلكترونية عبر نظم المعلومات وآفاق تطورها في تونس ومدى إمكانية تطبيقها في ليبيا، دراسة مقارنة بين بعض المؤسسات الليبية وبعض المؤسسات التونسية، رسالة لنيل درجة الماجستير من أكاديمية الدراسات العليا، مدرسة العلوم الإدارية والمالية، قسم إدارة الأعمال، طرابلس/ليبيا، خريف 2005، ص 64.

التي أنشأتها ولا يمكن فك شفرتها إلا باستخدام المفتاح العام العائد إليها ولهذا يطلق على اقتران التمويه المستخدم في إنشاء البصمة الالكترونية اسم آخر وهو اقتران التمويه الأحادي الاتجاه[336].

ثانيا: الخادم المفوض أو الموكل

يحتوي جهاز الخادم المفوض على كافة البرامج والبيانات التي تحتاجها الأجهزة الفرعية على الشبكة، حيث يقوم الخادم المفوض بدور الوسيط بين الشبكات المؤمنة والشبكات غير المؤمنة، وذلك لنقل ونسخ الملفات بين الأجهزة الفرعية أو العلمية، فعن طريقه يستطيع صاحب المنشأة رصد حركة موظفيه على شبكة المعلومات الدولية، ويمكن عن طريقه التحكم في عملية الدخول على مواقع معينة عن طريق إعطائه أمراً بعدم الدخول على مواقع معينة بذاتها، فعندما يحاول أحد العاملين الدخول على موقع من هذه المواقع يمنع الخادم المفوض تحقيق هذا المطلب، وغالبا ما يتم اقتران الحوائط النارية مع الخادم المفوض لضمان التحكم الكامل في عمليات الدخول والخروج وتحقيق التأمين الكامل للشبكات المؤمنة، فعندما يريد أحد العملاء إرسال ملف معين إلى عميل آخر يتم إرسال هذا الملف بداية للجهاز الخادم الذي يقوم بدوره إرساله إلى العميل الآخر[337]. وهو الخادم المفوض الذي تتعدد وظيفته في التحكم بعملية الدخول على المواقع الموجودة بالشبكات الخارجية من قبل العاملين بالشبكة الداخلية[338].

المبحث الثاني: توثيق معاملات الدفع الإلكتروني

تعتمد عمليات الدفع في التجارة الإلكترونية في إجراءاتها على شبكة اتصال مفتوحة، كما أن غالبية العقود التي تتم بين أطراف العلاقة تعد من العقود المبرمة بين غائبين، وذلك بسبب اختلاف مكان وزمان التعاقد وغياب التلاقي المباشر بينهم، عليه فإن توافر عنصري الأمان والثقة في الحالة هاته ليس مطلوباً فحسب، بل ضرورياً لتطوير أنظمة الدفع في التجارة الإلكترونية وتنمية المبادلات الاقتصادية[339]، لذلك ارتأت التشريعات الدولية والإقليمية والوطنية إيجاد وسيط (طرف ثالث) وظيفته توطيد العلاقات وتوثيقها بين الأشخاص الذين يعتمدون على الوسائط الإلكترونية (خاصة الذين يقومون بعمليات الدفع عبر شبكة الإنترنت) في إبرام تصرفاتهم. وبالتالي فإن رؤية المشرعين بضرورة إيجاد طرف محايد يؤكد أن التوقيع الإلكتروني

---

[336] عبد الرزاق نصر العجيلي، التجارة الإلكترونية عبر نظم المعلومات، المرجع السابق، ص 65.

[337] طارق عبد العال حماد، التجارة الالكترونية، بدون ذكر الطبعة، الدار الجامعية، الإسكندرية/مصر، ص 756.

[338] عبد الرزاق نصر العجيلي، التجارة الإلكترونية عبر نظم المعلومات، المرجع السابق، ص 69.

[339] أشارت العديد من الدراسات وكما سنرى في الباب الموالي إلى أن عدد حالات الغش والاحتيال التي تتم عبر شبكة الإنترنت في تزايد مضرد.

الخاص بعملية الدفع صادر عن صاحبه وأنه صحيح وأن البيانات الموقعة لم تُحور أثناء إرسالها، تعد خطوة ناجحة وأساسية في تطوير وانتشار التجارة الإلكترونية، إذ يربط هذا الوسيط هوية مرسل المحرر الإلكتروني بالمفتاح العام المقابل للمفتاح الخاص الذي به يوقع المحرر الإلكتروني، وذلك من خلال شهادة إلكترونية تحتوي مجموعة من البيانات من ضمنها المفتاح العام[340].

وهذا الوسيط يدعى بمزود خدمة التصديق الإلكتروني، تقوم مهمته على إصدار شهادات إلكترونية تعطي لتوقيع الإلكتروني ولمعاملات الدفع الإلكتروني مزيدا من المصداقية، وتكتسب خدمة المصادقة الإلكترونية أهمية كبيرة عندما ترتبط الشهادات التي تتعامل بها بمسائل دقيقة كالأموال، يطمئن كافة الأطراف المتعاملة إلى أن البيانات المتداولة والتوقيعات الواردة عليها صحيحة؛ فمثلا البائع (وبناء على صحة توقيع المشترى) سوف يرسل البضاعة للمشتري الذي بدوره (وبناء على صحة توقيع البائع) سوف يقوم بتسديد ثمن البضاعة المشتراة، كذلك فإن النظام المحاسبي الإلكتروني في البنوك وبناء على صحة توقيع حامل البطاقة أو صاحب الحساب سوف يتولى الدفع بالطريق الإلكتروني وتسوية الحسابات إلكترونياً دون تدخل حامل البطاقة أو موظف البنك[341].

وبالتالي يجب أن تتوفر الثقة والمصداقية في البيانات المتداولة خصوصاً تلك التي يكون موضوعها دفعاً مالياً وذلك عن طريق وسيط محايد يعطي شهادة رقمية أو وثيقة إلكترونية تشهد بصحة هذه البيانات، وهذا الوسيط هو شخص طبيعي أو معنوي مرخص له بممارسة هذه المهنة، ولهذه الغاية فقد شهدت السنوات الأخيرة زيادة في خدمات التصديق الإلكتروني على شبكة الانترنت من خلال عدة شركات تجارية نذكر منها (Web Trust) و(Verisign) و(Trust)[342]. إذ تقوم بإصدار شهادات رقمية تحقق توفيق معاملات الدفع الإلكتروني وكذا المعلومات الأخرى التي تتعلق بالتاجر.

وعليه، ومن أجل توثيق معاملات التجارة الإلكترونية عموماً والدفع الإلكتروني خاصة فإننا نحتاج إلى طرف ثالث مؤتمن وموثوق للتحقق من المعلومات التي يعتمد عليها كل نظام، باعتباره طرف حيادي (مزود

---

[340] عيسى غسان ربضي، القواعد الخاصة بالتوقيع الإلكتروني، المرجع السابق، ص112.

[341] جروج نهاد أبو جريش وخشان يوسف رشوان، المدخل إلى مصارف الانترنت، مرجع سابق، ص 59.

[342] وفي أستراليا طور معهد المحاسبين القانونيين نظاماً يستطيع من خلاله المحاسب القانوني أن يطلب تقييم موقع ويب لضمان التزامه ببعض المبادئ والمعايير، وهو نظام يسمح للموقع بأن يقدم تأكيد ضمان إحدى الشركات المعترف بها في أستراليا كما يسمح للمستهلكين الإطلاع إلى تقرير المحاسب القانوني، راجع سعيد أحمد إسماعيل، أساليب الحماية القانونية، لمعاملات التجارة الالكترونية، المرجع السابق، ص 270.

خدمة التصديق الالكتروني) يصدر عديد من الشهادات التي تتضمن قاعدة بيانات إلكترونية توفر جميع المعلومات الضرورية للموقع والغير، وبالتالي سنبحث عن الإطار القانوني لمزود لخدمة التصديق الإلكتروني (المطلب الأول) ومن ثم نتطرق لماهية الشهادات الإلكترونية التي تصدر عن هذا المزود (المطلب الثاني).

الفرع الأول: هيئات المصادقة الإلكترونية

طرحت عملية تبادل المعلومات المتعلقة بعمليات الدفع الإلكتروني عبر شبكة الانترنت مسألة المصادقة على التواقيع الإلكترونية، لدورها الواسع في نشر الآمان والموثوقية في مثل هذه التبادلات، الأمر الذي ينعكس إيجابياً على نسبة المتعاملين عبر شبكة الانترنت وأدى إلى تنامي العمليات المالية من خلال وسائل الدفع المختلفة، بشكل جعل معه العديد من التشريعات والقوانين تهتم بعملية تنظيم عمل الشخص الثالث أو مزود خدمة التصديق، ووضعت لها شروطاً لمزاولتها،

حيث هذه فرضت التشريعات التي نظمت عمل الجهة المختصة بإصدار شهادات التصديق الإلكترونية شروطاً مهنية يجب أن تتوفر في كل من يتقدم بطلب لترخيص مؤسسة أو شركة للعمل بمجال إصدار شهادات التصديق الإلكترونية، كما فرضت عليه واجبات يجب أن يلتزم بها خلال مدة صلاحية الترخيص، وفي حالة فقد المرخص له إحدى هذه الشروط أو أخل بإحدى الواجبات الملقاة على عاتقه فمن حق الجهة المانحة للتلخيص تعليق عمله أو إلغاء التلخيص الممنوح له[343]. كما نظمت هذه التشريعات شهادات التصديق الإلكترونية من حيث البيانات التي يجب أن تحتويها ومدى مصداقيتها.

الفقرة الأولى: التنظيم القانوني لهيئات خدمة التصديق

يتجلى التنظيم القانوني لمزود خدمة التصديق الإلكتروني من خلال عدة تعريفات قانونية للجهة المختصة بإصدار شهادات تصديق الإلكترونية، فقد عرفها قانون "الأونيسترال" النموذجي بشأن التوقيعات الإلكترونية وفق المادة الثانية فقرة (هـ) بأنها "شخص يصدر شهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية"، كما يعرف التوجيه الأوروبي رقم 1999/93 للتوقيعات الالكترونية مزود خدمات التصديق وفقاً للمادة الثانية فقرة (11) بأنها "الشخص الطبيعي أو الكيان القانوني الذي يصدر الشهادات أو يوفر الخدمات

---

[343] نصت المادة الثالثة من التوجيه الأوروبي بشأن التوقيعات الإلكترونية (الخاصة بسريان تطبيق التوجيه) على ما يلي:

" أ- على الدول الأعضاء ألا تخضع توريد خدمات التوثيق لأي ترخيص مسبق .

ب- تحسين مستوى خدمة التوثيق المقدمة، على أن تكون المعايير جميعها المتعلقة بهذه النظم موضوعية وشفافة وتناسبية وغير تميزية. كما أنه لا يمكن للدول الأعضاء أن تقيد عدد المكلفين بخدمة التوثيق لأسباب تتعلق بمجال تطبيق هذا التوجيه".

الأخرى المتعلقة بالتوقيعات الالكترونية[344]، أما الفصل الثاني من قانون المعاملات والتجارة الإلكترونية التونسي فقد عرفها بأنها "كل شخص طبيعي أو معنوي يحدث ويسلم ويتصرف في شهادات المصادقة ويسدي خدمات أخرى ذات علاقة بالإمضاء الإلكتروني"، أما قانون التجارة الإلكتروني البحريني فقد ميز بين مزود خدمات الشهادات ومزود خدمات شهادات المعتمد، وقصد بالأول من خلال مقتضيات المادة الأولى منه "الشخص الذي يصدر شهادات إثبات الهوية لأغراض التوقيعات الإلكترونية أو الذي يقدم خدمات أخرى تتعلق بهذه التوقيعات"، أما المقصود بمزود خدمات شهادات المعتمد فهو "مزود خدمة شهادات يتم اعتماده لإصدار شهادات معتمدة طبقاً لأحكام المادتين (16) و(17) من هذا القانون". وقد عرفتها اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري من خلال المادة الأولى فقرة (6) بأنها "الجهات المرخص لها بإصدار شهادة التصديق الإلكتروني وتقديم خدمات تتعلق بالتوقيع الإلكتروني. أما قانون المعاملات الإلكترونية الأردني فلم يورد أي تعريف للجهة المختصة بإصدار شهادات التصديق الإلكترونية، ويعزي ذلك إلى أن المشرع الأردني ترك تنظيم الأحكام الخاصة بعمل تلك الجهة للائحة تصدر لاحقاً (المادة 40/ب من قانون المعاملات الإلكترونية).

أما الفقه فقد عرف الجهة المختصة بإصدار شهادات التصديق الإلكترونية بأنها "هيئة (أم مؤسسة) يتولى إدارتها شخص طبيعي أو معنوي، تعمل بترخيص من إحدى مؤسسات الدولة، وظيفتها إصدار شهادات تصديق إلكتروني تربط بين شخص (طبيعي أو معنوي) ومفتاحه العام، أو أية مهمة أخرى تتعلق بالتوقيع الإلكتروني"، ويعرفها أيضا بأنها كل هيئة أو شخص طبيعي أو معنوي يصدر شهادات ويسلمها ويديرها أو يقدم أية خدمة أخرى لها علاقة باستعمال التوقيع الالكتروني[345]، وقد شبه الفقيه الفرنسي Bensoussan وظيفة الشخص الثالث بوظيفة كاتب العدل مما دفع البعض لتسمية الشخص الثالث المصادق بكاتب العدل الإلكتروني نظرا لنوع العمل الذي يؤديه، غير أن الفقيه Caprioli عارض الرأي السابق بقوله أن الشخص الثالث ليس مكاناً لإبداع العمل القانوني أو العقد المبرم بل للتأكد فقط من كون مفتاح التشفير العمومي أو التوقيع الإلكتروني يعود إلى من يجيزه فعلاً (أي حائز المفتاح الخصوصي ذاته). وهي اختلافات جعلت بعض التشريعات تذهب إلى وضع تعريف واضح لمزود خدمة التصديق الإلكتروني كما هو الحال بخصوص المشرع التونسي الذي وضح

---

[344] Article 2-11 : certification- service- provider, imeans an entity or alegal or natual person who issues certificates or provides other services related to electronic signatures.

[345] جورج نهاد أبو جريش وخشان يوسف رشوان، المدخل إلى مصارف الانترنت، مرجع سابق، ص 60.

ما المقصود بمزود خدمة التصديق الإلكتروني من خلال المواد (8-10) من القانون المتعلق بالتجارة الإلكترونية (المشار إليه أعلاه) بأنه الطرف الذي يسمى بالوكالة الوطنية للمصادقة الإلكترونية ويتمتع بالشخصية الاعتبارية والاستقلال المالي الإداري[346].

أما المشرع المغربي فقد أناط للوكالة الوطنية مهام السلطة الوطنية المكلفة بالمصادقة الالكترونية ومراقبة طرق التشفير من خلال المادة 15 من قانون 05-53 المتعلق بتبادل المعطيات القانونية، إلا أن المادة 43 من نفس القانون تنص على أنه "استثناء من أحكام الفقرة الأولى من المادة 21 أعلاه يمكن للحكومة باقتراح من السلطة الوطنية المشار إليها في المادة 15، وأخذ في الاعتبار مصلحة المرفق العام، اعتماد الأشخاص المعنوية للقانون العام من أجل إصدار شهادات إلكترونية مؤمنة، وتسليمها وتدبير الخدمات المتعلقة بها، وفق الشروط المنصوص عليها في هذا القانون والنصوص المتخذة لتطبيقه"، وهي مقتضيات يتضح من خلالها أن المشرع المغربي قد أعطى الحق للوكالة الوطنية بإصدار شهادات إلكترونية أو أشخاص تحددهم الحكومة باقتراح من الوكالة الوطنية نفسها، على أن يقع في المقابل على عاتق الشخص المصادق واجبات نصت عليها المادة (6)، وهذه الواجبات نص عليها الملحق الثاني من الإرشاد الأوروبي وتتمثل في تأكيد المعلومات، وتسليم الشهادات وحفظ سجل معلوماتي، بالإضافة إلى المحافظة على سرية البيانات ذات الطابع الشخصي وحمايتها واستعمال وسائل تقنية آمنة وأنظمة موثوقة للتعريف بهوية الموقع[347].

كما يفترض بكل شخص مصادق يرغب بإصدار شهادات موصوفة في ظل التشريع الأوروبي أن يراعى عند إصداره هذه الشهادات، أحكام الملحق الثالث من الإرشاد الأوروبي وكذلك الملحق الرابع التي تصب جميعها في تأمين درجة آمان عالية لآلية المصادقة، وكل هذه الواجبات تشكل ركائز أساسية لتعزيز الثقة في البيئة المعلوماتية لاسيما فيما يتعلق بمعاملات الدفع الإلكتروني حيث يطمئن المتعاملون لهوية بعضهم وإلى خصوصية أعمالهم.

الفقرة الثانية: شروط وواجبات مزودي خدمات التصديق الإلكتروني

نظراً لاختلاف أحكام التشريعات المنظمة لمزودي خدمات التصديق الإلكتروني، فإنه سوف نبحث الحد المعقول من الشروط والواجبات التي يجب على كل مزود الالتزام بها، ذلك لأن الهدف الرئيسي من إنشاء

[346] عبد الفتاح بيومي حجازي، مقدمة في التجارة الإلكترونية العربية، مرجع سابق، ص 128.

[347] جورج نهاد أبو جريش وخشان يوسف رشوان، المدخل إلى مصارف الانترنت، المرجع السابق، ص 60.

جهات مختصة بإصدار شهادات تصديق إلكترونية هو تمكين المرسل إليه من التأكيد من هوية المرسل وصلاحية توقيعه الرقمي، فهذا الأخير يتكون من مفتاحين عام وخاص لا يرتبطان ماديا بشخصية صاحبهما، فكيف يطمئن المرسل إليه إلى أن المفتاح العام الذي بحوزته تعود ملكيته للمرسل وليس لشخص آخر؟

في الواقع العملي عندما يرسل شخص محرراً إلكترونياً إلى شخص آخر يرفق به ما يعرف بهويته، وغالبا (وبما أن الاتصال يتم إلكترونياً) ما يبعث شهادة إلكترونية تحتوي مجموعة من البيانات من ضمنها ما يحدد للمرسل إليه هوية المرسل وسلطاته في التوقيع، وبعد أن يتأكد المرسل إليه من صلاحية الشهادة الإلكترونية المرسلة له (من خلال الجهة التي أصدرتها) يعول على المحرر الإلكتروني، وهكذا يتم التبادل بين المرسل والمرسل إليه إلى أن يتوصلا إلى اتفاق نهائي.

إذن من واجبات الجهة المختصة بإصدار شهادات التصديق الإلكترونية، إصدار شهادة إلكترونية تحدد هوية الموقع (المرسل) وصلاحية توقيعه، ولكن لكي تقوم جهة الإصدار بهذا الواجب يجب أن تكون حاصلة على ترخيص مسبق من إحدى مؤسسات الدولة، وحسب كل من المشرع المغربي (طبقاً بما جاء به القانون 05-53 المتعلق بتبادل البيانات) وقانون تنظيم التوقيع الإلكتروني المصري، لا يجوز لأي شخص طبيعي أو معنوي مزاولة مهنة مزودي خدمة المصادقة وإصدار شهادات التصديق الإلكتروني (داخل البلاد أو خارجها) أو حتى العمل في مجال الخدمات الوسيطة في التجارة الإلكترونية، شرط الحصول على ترخيص من الجهة المختصة بذلك (الوكالة الوطنية بالنسبة للمملكة المغربية وهيئة صناعة تكنولوجيا المعلومات بالنسب لجمهورية مصر)، وقد أحسن كل من المشروعين المغربي والمصري عملا عندما أقرا لهاته الجهات المختصة بمتابعة ومراقبة أعمال المرخص لهم بإصدار شهادات التصديق أو تعليقه إذا خالفت الجهة المرخص لها إصدار شهادات التصديق شروط الترخيص. أما المادة (40/ه) من قانون المعاملات الإلكترونية الأردني فقد أناطت بمجلس الوزراء إصدار الإجراءات المتعلقة بأعمال الجهة المختصة بإصدار شهادات التصديق. ويضاف لشرط الحصول على ترخيص مسبق، شروط أخرى تناولته التوجيهة الأوروبية في ملحقها الثاني[348]، (الخاص بمزودي خدمة التصديق الذين يصدرون شهادات مصادقة إلكترونية) يمكن إجمالها في وجوب منح الثقة الضرورية لتزويد خدمات التصديق، إذ لا يمكن لأي شخص طبيعي أو اعتباري أن يمارس نشاط مزودي خدمات المصادقة الإلكترونية دون الحصول على الثقة الضرورية والترخيص لمزاولتها، ويضمن عملية تقديم المعلومات الفورية مباشرة وبشكل آمن،

---

[348] En Ocialjoumal of the European communities, 19-1-2000, L13/20.

وخدمة إلغاء آمنة وفورية، وكذا يضمن بأن التاريخ والوقت لصدور الشهادة أو إلغائها يمكن أن يحدد بالضبط، كما يقع على عاتقه القيام بالتحقق من الهوية الشخصية بالوسائل الملائمة طبقا للقانون الوطني، والمزايا الخاصة بالشخص الذي ستصدر له الشهادة، إذا كانت قابلة للتطبيق، لذلك يجب أن يمتلك الموظفون المستخدمون لخدمة التصديق المعرفة التخصصية والتجربة والمؤهلات الضرورية، وبشكل خاص الكفاءة في المجالات الإدارية والخبرة في تقنية التوقيع الإلكتروني وإجراءات الأمن الصحيحة والمألوفة، ويجب أن يطبقوا الإجراءات الإدارية المطابقة والملائمة للمعايير القياسية[349].

ومن واجبات مزودي التصديق والمختص بإصدار شهادات التصديق الإلكترونية، الالتزام بالبيانات المقدمة له من أصحاب الشأن، حيث يحضر عليه حذف أو تعديل أو إضافة أي بيان من البيانات المقدمة إليه[350]، وهذا ما يعرف بمعالجة البيانات الإلكترونية، وقد منعت التشريعات المختلفة الجهة المختصة بإصدار شهادة التصديق الإلكترونية من إجراء هذه المعالجة من تلقاء نفسها، ويشترط عليها أيضاً استعمال أنظمة ومنتجات جديرة بالثقة لمنع إدخال أي تعديل وتضمين عملية التشفير التقني المزودة من قبلهم، وتوفير المعايير الضرورية للحماية من تزوير الشهادات، وعندما ينتج مزود خدمة التصديق توقيع مبتكر للبيانات يجب أن يضمن السرية أثناء عملية إنشاء مثل هذه البيانات، ويستلزم على مزودي خدمات التصديق تسجيل كل المعلومات ذات الصلة بشهادة المصادقة الإلكترونية ولفترة زمنية مناسبة، وبشكل خاص لغرض الإثبات وتزويد الشهادة بالدليل طبقاً للإجراءات القانونية لأن مثل هذا التسجيل قد يتم بشكل إلكتروني، إضافة إلى عدم تخزين أو نسخ بيانات إنشاء توقيع الشخص الذي يزود من قبل مقدم خدمة التصديق بمفتاح الخدمات الإدارية.

وكذلك يلتزم مزود خدمات التصديق والمختص بإصدار شهادات المصادقة الإلكترونية بالمبادئ والسياسات التي أعلن عنها في مواثيقه أو نشراته لإدارة نشاطه[351]، ومن واجبات هذا المزود أيضاً أن يوفر لمن يعول على الشهادة الإلكترونية، الوسائل التي تؤكد له أن الموقع محدد الهوية في الشهادة، وكان لديه (وقت التوقيع) السيطرة على الأداة الفنية اللازمة للتوقيع وأنها كانت وقت التوقيع سارية المفعول، وقد طبق قانون المبادلات والتجارة الإلكترونية التونسي ذلك بأن ألزم كل مزود لخدمات التصديق الإلكتروني بمسك سجل إلكتروني

---

[349] محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الالكترونية، مرجع سابق، ص 279.

[350] المادة (24/1/أ) من قانون المعاملات والتجارة الإلكترونية لإمارة دبي.

[351] المادة (9/أ) من قانون "الأونيسترال" النموذجي بشأن التوقيعات الإلكترونية، والمادة (24/أ/1/أ) من قانون المعاملات والتجارة الإلكترونية لإمارة دبي.

يدون به الشهادات التي يصدرها، وتمكين الأشخاص من الاطلاع إلكترونياً وبصفة مستمرة على البيانات المدونة به، وأيضاً من الوجبات المفروضة على مزود خدمات التصديق والمختص بإصدار شهادات المصادقة الإلكترونية حفظ الهوية الحقيقية للشخص الذي تقدم بطلب لإصدار شهادة تصديق إلكترونية، إذا رغب بإصدارها باسم مستعار[352]،

وقبل الدخول في علاقة تعاقدية مع هذا شخص الذي يطلب تزويده بشهادة توقيع الكتروني، يبلغ بأنه سيتحمل الشروط والتعابير الدقيقة لوسائل الاتصال بخصوص استعمال الشهادة، ويتضمن ذلك أي تقييدات على استعمالها يمكن أن ترسل الكترونياً مع وجوب أن تكون مكتوبة بلغة سهلة ومفهومة[353].

المطلب الثاني: شهادات المصادقة الإلكترونية

تصدر جهات التصديق الإلكتروني شهادة إلكترونية وظيفتها الربط بين الموقع ومفتاحه العام، وهي سجل إلكتروني يتكون من بيانات أو معلومات إلكترونية تنشأ وتعالج بواسطة وسيط إلكتروني، وتحتوي كل شهادة بيانات خاصة بصاحبها كاسمه (سواء الحقيقي أم المستعار) وسلطته في التوقيع وأهليته ومهنته[354]...، لذلك تعد شهادة المصادقة الإلكترونية واجبة لممارسة التجارة الإلكترونية عموماً والوفاء عبر شبكة الانترنت خاصةً، كونها تعتبر بمثابة جواز سفر وعن طريقها يتحدد شخصية طرفا التعاقد ويأمن كلاهما أن التوقيع الوارد على المستند يخص المتعاقد الآخر، وتبدو أهمية هذه الشهادة في أنها تسمح لمواقع الشبكة بالتعرف على المستخدم الذي يمتلكها (شهادة المصادقة الإلكترونية)،

إذ يمكن لمزودات هذه المواقع من الوصول إلى المعلومات الخاصة والمحمية التي تتضمنها، وقد يكون مثالها العمليات البنكية التي تحتاج لشهادات رقمية عالية في درجة الآمان، ولعل أكثر مثال توضيحي التطبيق هو عميل البنك الذي يمكن له من خلال شهادة التعريف الرقمية النفاذ إلى حساباته وبياناته المالية، والقيام بالعمليات الممكنة في بيئة آمنة ومضمونة ولا تحتاج صلاحية استخدامها في مجال التسوق الالكتروني بقدر

---

[352] وقد أجازت المادة (7/أ) من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري، استخدام اسم مستعار أو اسم الشهرة عند تقديم طلب استخراج شهادة تصديق إلكترونية.

[353] محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الالكترونية، مرجع سابق، ص 280.

[354] إن الشهادة الإلكترونية محددة بموجب التوصية (x.509) الصادرة عن الاتحاد الدولي للاتصالات اللاسلكية (ITU)، وتكرر الأخذ بهذه التوصية من جانب التنظيم الخاص بعالم الإنترنت تحت عنوان Internet Engineering Task Force الذي طوع المعيار الخاص بالشهادات الإلكترونية في سبيل تطبيقه على تكنولوجيا التوقيع الإلكتروني. راجع في هذا: عيسى غسان ربضي، القواعد الخاصة بالتوقيع الإلكتروني، المرجع السابق، ص126.

ما تحتاج إلى المستوى الأدنى الخاص بشهادة التعريف الشخصية وبيان الدور الذي تقوم به، إذ أنها تساعد في تشفير الرسائل الالكترونية وفك تشفيرها[355].

وتعددت التعريفات الإيضاحية لشهادة التصديق الإلكترونية، كما تعددت تسمياتها، وذلك لتعدد التشريعات والقوانين التي نظمت التجارة الإلكترونية ومعاملات الدفع الإلكتروني. فلما لشهادة المصادقة من دور فعال في إبرام التصرفات عبر الوسائط الإلكترونية خاصة في مجال الإثبات، اعتنى المشرعون بأهميتها، ولذلك ارتأوا أنه من الضروري إيضاح المقصود بشهادة المصادقة الإلكترونية خوفاً من حدوث اللبس في تحديد المقصود بها أو في وظيفتها، فلقد عرفت المادة (2/ب) من قانون "الأنيسترال" النموذجي بشأن التوقيعات الإلكترونية شهادة التصديق الإلكترونية بأنها "رسالة بيانات أو سجل يؤكدان الارتباط بين الموقع وبيانات إنشاء التوقيع"، أما المادة (2) من التوجيه الأوروبي بشأن التوقيعات الإلكترونية الصادر في 13 ديسمبر 1999 فقد ميزت في الفقرتين التاسعة والعاشرة بين الشهادة الإلكترونية البسيطة والشهادة الإلكترونية الموصوفة، وعرفت الأولى بأنها "الشهادة الإلكترونية التي تربط البيانات الخاصة بفحص التوقيع الإلكتروني وشخص معين وتؤكد هوية هذا الشخص"، أما الشهادة الثانية فقد عرفتها بأنها "شهادة تستوفي المتطلبات المنصوص عليها في الملحق الأول، والتي يقدمها المكلف بخدمة التوثيق المستوفي للمتطلبات المنصوص عليها في الملحق الثاني"[356].

ولقد عرف القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية من خلال الفصل الثاني، شهادة المصادقة الإلكترونية بأنها "الوثيقة الإلكترونية المؤمنة بواسطة الإمضاء الإلكتروني للشخص الذي أصدرها والذي يشهد من خلالها أثر المعاينة على صحة البيانات التي تتضمنها"، وعرفها قانون إمارة دبي الخاص بالمعاملات والتجارة الإلكترونية في المادة الثانية بأنها "شهادة يصدرها مزود خدمات التصديق يفيد فيها تأكيد هوية الشخص أو الجهة الحائزة على أداة توقيع معينة ويشار إليها في هذا القانون (بالشهادة)، وإذا أمعنا النظر في هذه التعريفات نجد أنها اتكأت جميعها في تعريفها لشهادة المصادقة الإلكترونية على الجانب الوظيفي لهذه الشهادة، وهذا راجع في نظري للدور الذي تقوم به في مجال معاملات التجارة الإلكترونية.[357]

---

[355] عدنان الحسيني، شهادات التعريف الرقمية والتجارة الإلكترونية، بحث منشور لدى مجلة انترنت العالم العربي: عدد فبراير 1999 على موقع الكتروني .www.jawmg.ca.ae

[356] وقد أورد المرسوم الفرنسي رقم 2001-272 في 30 مارس 2001 الباب 3 والقانون الألماني للتوقيعات الرقمية ذات التعريف.

[357] للمزيد من التعريفات أنظر المادة (1/و) من قانون تنظيم التوقيع الإلكتروني المصري، والمادة (2) من قانون المعاملات الإلكترونية الأردني، والمادة (2) من قانون التجارة الإلكترونية البحريني.

الفقرة الأولى: مضمون شهادة المصادقة الإلكترونية

أقرت بعض التشريعات نموذجين للشهادات الإلكترونية هما الشهادة الإلكترونية البسيطة والشهادة الإلكترونية الموصوفة، وهذه الأخيرة (لكي تكتسب صفة الشهادة الموصوفة) يجب أن تستجيب لسلسلة من المعايير، مثل أن تصدر من جهة خاصة بإصدار شهادات التصديق وأن تحوي مجموعة من البيانات التي حددتها التشريعات التي نظمت التجارة الإلكترونية أو الدفع الإلكتروني، أما شهادة التصديق البسيطة فهي حسب التوصية (X.509) الصادرة عن الاتحاد الدولي للاتصالات (ITU) فتشتمل على نوعين من البيانات وهي البيانات الإلزامية (التي يجب على كل شهادة أن تحتويها) والبيانات الاختيارية التي ترك لكل جهة مختصة بإصدار شهادات إلكترونية حرية الالتزام بها، فيحب أن تحتوي شهادة المصادقة الإلكترونية الموصوفة والمعترف بها في مختلف القوانين والجديرة بالثقة والتعامل بها، على بعض المعلومات الخاصة بالموقع، فتزايد عدد العملاء على شبكة الانترنت بسرعة وقيامهم بإدخال أسماء أو ألقاب خاصة بكل شخص ستؤدي إلى الالتباس فيما بينهم، لذلك يجب أن تتضمن هذه الشهادة بيان يفيد هوية صحبها (ببيان اسمه ولقبه وعمله ومحل إقامته والبيانات الأخرى التي تشير إلى أنه صاحب هذه الشهادة)، وهوية الشخص الذي أصدرها وإمضائه الإلكتروني، وأضاف التوجيه الأوروبي واللائحة التنفيذية المصرية إلى هذا البيان البلد الذي تقيم به هذه الجهة[358] ، ويوفر هذا البيان الطمأنينة للطرف الذي يعتمد على الشهادة الإلكترونية خاصة وأن الجهة المصدرة مسؤولة عن الأضرار التي تلحق بالمعتمدين على الشهادة، كل ذلك حتى يمكن تحديد المسؤولية القانونية للشخص المصدر وما إذا كان مرخصاً له أم لا، وكذلك فقد يسأل قانوناً في حالة تسريب منظومة فك الشفرة الخاصة ببيانات الشهادة، ولهذا لا بد من أن يكون اسمه معلوماً حتى يمكن تحديد مسؤوليته القانونية إذا اقتضى الأمر ذلك[359].

كما يقع على عاتقه توضيح مجالات استعمال شهادة المصادقة والغرض الذي لأجله صدرت، سواء كانت تصديقاً على توقيع إلكتروني أو على منظومة إحداثه، فالشهادات الصادرة عن مزود الخدمة كثيرة ومتنوعة وذلك حسب أغراضها ويجب أن تتوفر على نظام فني يحكم شروط إصدارها، وهو منظم من خلال عناصر التدقيق في توقيع صاحب الشهادة التي يتم الرجوع إليها لتأكد من ضمان صحة التواقيع الإلكترونية لصاحب هذه الشهادة، كما يجب الإشارة إلى بيان يحدد بداية ونهاية صلاحية الشهادة الإلكترونية، وهذا البيان يحدد

[358] المادة (ب) من الملحق الأول، والمادة (3/20) من اللائحة.

[359] عبد الفتاح بيومي حجازي، مقدمة في التجارة الإلكترونية العربية، المرجع السابق، ص 167.

النطاق الزمني لمسؤولية الجهة التي أصدرت الشهادة، فتحسباً لتغير البيانات التي يقدمها الأشخاص لجهة التصديق تعمد هذه الأخيرة إلى تحديد نطاق زمني تضمن به صحة البيانات الواردة في الشهادة حتى يكون المتعاملون مع صاحب الشهادة في مأمن من التعامل مع شخص ليسوا متأكدين من صحة البيانات الخاصة به، وهي بيانات تتعلق بعمليات تجارية ترتب آثارا مالية وقانونية كبيرة في حق الأطراف، ولذلك فسريان الشهادة هو بيان للأطراف المتعاملة سيما لو تعلق الأمر بالمركز المالي للشخص أو شركة أو أصول هذه الشركات ونشاطها وغيرها من البيانات التي يعول عليها، لذلك يجب على صاحب الشهادة بأن يقوم بتزويد مزود الخدمة، وبصفة دائمة أي تغيير يطرأ على بياناته المدونة في الشهادة، حتى يقوم (مزود الخدمة) بتغيير بيانات الشهادة وإخطار ذوي الشأن بذلك التغيير.

وفي هذا الصدد جاء المشرع المغربي في المادة (11) من القانون رقم 53-05 المتعلق بالتبادل الالكتروني للمعطيات القانونية بمجموعة من البيانات التي يجب أن تتضمنها شهادات المصادقة الإلكترونية وهي على النحو التالي:

أ. الإشارة إلى هذه الشهادة مسلمة باعتبارها شهادة إلكترونية مؤمنة.

ب. هوية مقدم خدمات المصادقة الإلكترونية وكذا اسم الدولة التي يوجد مقره بها.

ج. اسم الموقع صاحب الشهادة الإلكترونية المؤمنة أو اسمه المستعار عند وجوده، وفي هذه الحالة الأخيرة يتعين التعريف بهذه الصفة.

د. المعطيات التي تمكن من التحقق من التوقيع الالكتروني المؤمن.

ه. تحديد بداية ونهاية مدة صلاحية الشهادة الإلكترونية.

و. الرقم السري للشهادة الإلكترونية.

ز. التوقيع الإلكتروني المؤمن لمقدم خدمات المصادقة الإلكترونية الذي يسلم الشهادة الإلكترونية.

ح. عند الاقتضاء، شروط استخدام الشهادة الإلكترونية ولا سيما المبلغ الأقصى للمعاملات التي يمكن أن تستخدم فيها الشهادة المذكورة.

يتضح من خلال مقتضيات هذه المادة أنها قد تضمنت جل البيانات الواجب توفرها في الشهادة الإلكترونية، بما فيها تحديد قيمة استخدام الشهادة الإلكترونية ونوع التعاملات[360]، أما فيما يزيد على

[360] المادة (و) من الملحق الأول للتوجيهية الأوروبي، والمادة (6/ز) من مرسوم 30 مارس 2001، والمادة (3-10/20) من اللائحة التنفيذية المصرية.

النصاب المذكور بالشهادة أو التعدي عن نوع التصرف الذي من أجله صدرت الشهادة، لا تسأل عنه الجهة التي أصدرت الشهادة ويعد إهمالاً وتقصيراً من الشخص الذي اعتمد على الشهادة، وأخيراً أشارت إلى بيان تحقيق التوقيع الإلكتروني المقابل لبيان إنشائه[361]، ويتمثل هذا البيان بالمفتاح العام لصاحب الشهادة.

وإلى جانب هذه البيانات الإلزامية التي نصت عليها هذه المادة ومعظم التشريعات التي نظمت أحكامها نشاط مزودي خدمات المصادقة الإلكترونية، هناك العديد من البيانات اعتادت بعض الجهات إضافتها إلى البيانات الأساسية كرقم إصدار الشهادة الإلكترونية ورقم مزاولة نشاط تقديم خدمة التصديق الإلكتروني واسم الجهة المانحة للترخيص، ويمنع غير ذوي الصفة القانونية من إجراء أي تعديل أو إلغاء أي من البيانات الأساسية أو التي تضيفها الجهات المذكورة أعلاه.

الفقرة الثانية: حجية شهادات المصادقة الإلكترونية في إثبات الدعوى المصرفية

تصدر جهات التصديق الإلكتروني شهادة إلكترونية وظيفتها الربط بين الموقع ومفتاحه العام، وهي (كما سبقت الإشارة) سجل إلكتروني يتكون من بيانات أو معلومات إلكترونية تنشأ وتعالج بواسطة وسيط إلكتروني، وتحتوي كل شهادة على بيانات خاصة بصاحبها كاسمه وسلطته في التوقيع وأهليته ومهنته، وبما أن الشهادة الإلكترونية متاحة للجميع فإنها تتمتع بحجية كاملة داخل حدود الدولة التي صدرت فيها وذلك بالاستناد إلى مبدأ التكافؤ الوظيفي إذ تقوم هذه الشهادة بالتصديق على المستندات الورقية والتوقيعات الخطية[362] هذا من ناحية، ومن ناحية أخرى فإن الجهات الحكومية المختصة ستتولى مهمة الإشراف والرقابة على سلطات التصديق، وهي الرقابة التي قد تتم مباشرة أو بمناسبة كل منازعة تتعلق بنشاط المكلف بالتوثيق سواء من طرف السلطة العامة بالتصديق أو من خلال تخصيصها لجهات حكومية للقيام بوظائف سلطات التصديق وإصدار شهادات مصادقة إلكترونية.

أما فيما يتعلق بحجية شهادة المصادقة الإلكترونية على المستوى الدولي، فقد نظم القانون النموذجي بشأن التوقيعات الإلكترونية مسألة الاعتراف بالشهادات والتوقيعات الإلكترونية الأجنبية، إذ جاء في الفقرة

---

[361] المادة (ز) من الملحق الثاني من التوجيهية الأوروبي، والمادة (6/م) من مرسوم 30 مارس 2001، والمادة (6/20) من اللائحة التنفيذية.

[362] أن الشهادة الالكترونية محددة بموجب التوصية (x.509) الصادرة عن الاتحاد الدولي للاتصالات اللاسلكية (ITU) وتكرر الأخذ بهذه التوصية من جانب التنظيم الخاص بعالم (الانترنت) تحت عنوان (Internet Engineering task force) الذي طوع المعيار الخاص بالشهادات الالكترونية في سبيل تطبيقه على تكنولوجيا التوقيع الرقمي، راجع في هذا عيسى غسان ربطي: القواعد الخاصة بالتوقيع الالكتروني، دار الثقافة للنشر والتوزيع، الطبعة الثانية-عمان/الأردن لسنة 2012 ص 126.

الثانية من هذا القانون لتنص على الحد الأدنى للتكافؤ التقني للشهادات الأجنبية الذي يستند إلى اختبار الموثوقية على أساس الشروط التي تضعها الدولة المشترعة للتوثيق عملاً بالقانون النموذجي، وهو معيار ينبغي أن يطبق دون اعتبار لمتطلبات التصديق المطبقة في الدولة التي صدرت فيها الشهادة أو التوقيع الإلكتروني، وهذا ما قد نجده مختلفاً في الممارسة العملية التي نجد فيها أن سلطات التصديق تصدر شهادات ذات مستويات متفاوتة من الموثوقية، وفقاً للغرض الذي يقصد الزبائن أن يستخدموا الشهادات فيه، وطبقاً لمستوى موثوقية كل شهادة على حدة، ليست كل الشهادات جديرة بإحداث مفعول قانوني سواء داخليا أم في الخارج، وأن التكافؤ الذي يلزم إثباته هو التكافؤ بين الشهادات التي من نفس النوع[363]، وفي هذا الصدد نصت المادة (12) من القانون النموذجي المتعلق بالتوقيعات الإلكترونية على ما يلي:

1. لدى تقرير ما إذا كانت الشهادة أو التوقيع الإلكتروني ساري المفعول قانونيا أو مدى كونهما كذلك، لا يولى أي اعتبار إلى:
   أ. الموقع الجغرافي الذي تصدر فيه الشهادات أو ينشا آو يستخدم في التوقيع الإلكتروني
   ب. الموقع الجغرافي لمكان عمل المصدر أو الموقع.
2. يكون للشهادة التي تصدر خارج الدولة المشترعة نفس المفعول القانوني في الدولة المشترعة الذي للشهادة التي تصدر في الدولة المشترعة إذا كانت تتيح مستوى مكافئاً جوهرياً من الموثوقية.
3. يكون للتوقيع الإلكتروني الذي ينشأ أو يستخدم خارج الدولة المشترعة نفس المفعول القانوني في الدولة المشترعة الذي للتوقيع الإلكتروني الذي ينشا أو يستخدم في الدولة المشترعة إذا كان يتيح مستوى مكافئا جوهريا من الموثوقية.
4. لدى تقرير ما إذا كانت الشهادة أو التوقيع الإلكتروني يتيحان مستوى مكافئاً جوهرياً من الموثوقية لأغراض الفقرتين(2) أو(3) يولى الاعتبار للمعايير الدولية المعترف بها وإلى أي عوامل أخرى ذات الصلة.
5. إذا اتفقا الأطراف فيما بينهم، برغم ما ورد في الفقرات (2) و(3) و(4) على استخدام أنواع معينة من التوقيعات الإلكترونية أو الشهادات، يتعين الاعتراف بذلك الاتفاق باعتباره كافياً لأغراض الاعتراف عبر الحدود، ما لم يكن من شأن ذلك الاتفاق أن يكون غير صحيح أو غير ساري المفعول بمقتضى القانون الذي يتم تطبيقه في هده الحالة.

---

[363] محمد سعيد احمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الالكترونية، المرجع السابق، ص294.

يتضح من خلال قراءة مقتضيات هذه المادة أنها أعطت الحجية القانونية لشهادات التصديق الإلكتروني بتبنيها قاعدة عدم التمييز التي مفادها أن مكان المنشأ للشهادة يجب أن لا يكون عاملاً يحدد إلى أي مدى ينبغي الاعتراف بالشهادات أو التوقيعات الإلكترونية الأجنبية باعتبارها سارية المفعول قانونا، كما لا ينبغي تحديد ما إذا كانت الشهادة سارية المفعول قانوناً ولا إيلاء أهمية للمكان الذي صدرت فيه بل على موثقيتها التقنية.

وبقي لنا أن نشير بأنه توجد بعض المشاكل العملية المثارة بشأن الإثبات الإلكتروني في الدعوى المصرفية وما يتصل بها من مسائل إجرائية تتعلق بأمن المعلومات، فلقد جاء في لقاء مجموعة الخبراء الأوروبيين القانونيين (المناط بهم وضع التصور للدليل الإرشادي حول حجية سجلات الكمبيوتر والرسائل الإلكترونية المنعقد عام 1997) أن الحلول الإلكترونية في بيئة العمل البنكي لا يتعين أن تكون عبئا إضافياً للحلول الورقية القائمة، إذ أن اعتماد العمل المصرفي على التقنيات الحديثة المتعددة المحتوى والأداء والغرض، لا يجب أن يكون بحال من الأحوال وسيلة مضافة للأنماط التقليدية للعمل، تسير معها لتكون في الحقيقة أمام آليتين لإدارة العمل وتوثيقه، إحداها تعتمد التقنية بما تتميز به سرعة في الأداء وكفاءة في المخرجات وربما تكاليف اقل، وثانيهما استمرار الاعتماد على الورق وعلى وسائل العمل التقليدية غير المؤتمتة، ليبقى مخزون الورق هو المخزون الاستراتيجي للعمليات البنكية تنفيذاً وإثباتاً وتقييماً. وهذه الحقيقة تضعنا أمام أهم مشكلات الإثبات بالوسائل التقنية، إلا وهي مشكلة مدى قبول هذه الوسائل من قبل القطاعات المتعاملة بالأنشطة التجارية والمالية سواء الأفراد (الزبائن) أو مؤسسات الأعمال، فالقاعدة الأساسية التي يمكن الانطلاق منها تكمن في مدى الاطمئنان لسلامة الوسائل الإلكترونية في التعاقد والإثبات، وهذا يعتمد بشكل رئيس على ثلاثة عناصر أساسية الأول هو المكانيزم المستخدم ومحتوى التقنية والقدرة على تبسيط الفكرة وإيصالها للمتعاملين، والثاني يكمن في مدى كفاءة نظام التراسل الإلكتروني والثالث يتعلق بالثقافة والتأهيل للتعامل مع مشكلات هذا التراسل. ويضاف إلى هذا إن النظم التقنية المؤهلة يجب أن تكون قادرة على بناء الثقة بالوسائل الإلكترونية الحديثة للتعاقد والإثبات في الحقل البنكي أو في غيره من حقول النشاط التجاري والمالي، إذ يجب أن تكون بسيطة البناء محصنة من الاعتداء على المحتوى المعلوماتي سواء من داخل المنشاة أو خارجها، المنسجمة من حيث طريقة الأداء والمخرجات مع المستقر والسائد من معايير ومواصفات تقنية، المؤهلة للاستمرار في العمل دائما دون انقطاع أو خلل، وإذا كان ثمة اهتمام لدى المؤسسات المالية بحداثة النظم ودقتها وكفاءتها من حيث السرعة وسعات التخزين فما كان بأمن النظم وأمن المعلومات أن يسير بالقدر ذاته،

نظراً لما يشهده قطاع أمن المعلومات من تطوير بالغ وتغيرات متتالية، ليس في الوسائل المعتمدة لتوفير أمن المعلومات فحسب بل حتى في النظريات التي يرتكز عليها أمن المعلومات.

الخاتمة

ان تجربتنا البحثية المتواضعة مرت على حالات عملية (خاصة المؤسسات العاملة في ليبيا) أظهرت غياب استراتيجيات شاملة ودقيقة للتعامل مع أمن نظم المعلومات والبيانات المتبادلة، إذ تنطلق كثير من خطط حماية البيانات ووسائل تبادلها من نماذج مستوردة قد لا تراعي خصوصيات المؤسسة وخصوصيات القواعد المعلوماتية فيها وخصوصيات التوظيف ومحدداته والثقافة السائدة، لهذا كانت انجح الاستراتيجيات تلك القائمة على تطوير وسائل الأمن الداخلية المراعية للاعتبارات المذكورة، ولا نبالغ أن أحد أهم أسباب فشل وسائل حماية نظم وأمن المعلومات حتى في المؤسسات الكبرى يرجع إلى عدم إدراك الاحتياجات الواقعية للمؤسسة وعدم مراعاة تباين النماذج الجاهزة مع الواقع الفعلي للمؤسسة، ويرتبط بكفاءة النظم كفاءة المتعاملين معها وكفاءة مزودي الخدمات المتصلة بها داخليين كانوا أم خارجيين عن المنشأة، ومن هنا تكمن أهمية وظائف مستشاري النظم ومراقبي الأداء ووظائف مطوري النظم المناط بهم التواصل مع كل جديد والانفتاح على احتمالات الفشل والإخفاق بنفس القدر من الانفتاح على احتمالات النجاح والتميز.

الامن السيبراني ضرورة حتمية لازدهار التجارة الالكترونية

الدكتورة ايمان خليل

اختصاص عقود مدنية و تجارية، جامعة ابن خلدون

تيارت ،الجزائر

Gmail :imanekhelillabotiaret@gmail.com

الملخص:

في عصر العالم الرقمي ، تمثل التجارة الالكترونية أحد أهم مكونات الأعمال الاقتصادية عبر الإنترنت و التي تستوجب خلق بيئة موثوق بها حيث يمكن للعملاء الشعور بالثقة عند إجراء عمليات الشراء، أين تتم مشاركة بيانات الملايين من الأشخاص ، خاصة أثناء المعاملات عبر الإنترنت ، حيث يتضمن ذلك معلومات حساسة مثل أرقام بطاقات الائتمان وأرقام التعريف الشخصية وبيانات اعتماد تسجيل الدخول التي يجب أن تكون آمنة ما يستدعي ضرورة تطبيق الأمن السيبراني فالترابط الوثيق بين التجارة الالكترونية والامن السيبراني؛ يتضح جليًّا في الهجمات السيبرانية. حيث من خلالها يمكن سرقة بيانات بطاقات الائتمان من مواقع التجارة الإلكترونية. ناهيك عن تقويض ثقة الشركات والمستهلكين في ذلك النوع من التجارة .

تتمثل أهمية الموضوع في أن هناك علاقة وطيدة بين الامن السيبراني و التجارة الالكترونية فتراجع فعالية الأمن السيبراني يزيد من التكلفة المتكبدة إلى حد تقويض ثقة المستهلكين والشركات في التجارة الرقمية. ومن ثم، تتطلب تدابير الحماية تعاونًا دوليًّا بين القطاعين العام والخاص، نظرًا لاعتماد الشبكات، والمؤسسات، وسلاسل التوريد العالمية على نفس الأنظمة والبرامج التي توفر الشركات معظمها، وهو ما يعني وجود مخاطر مشتركة.

الكلمات المفتاحية: الامن السبراني ،العقد الالكتروني ،التجارة الالكترونية ،القانون الدولي ،الجريمة السبرانية .

Summary :

In the era of the digital world, electronic commerce represents one of the most important components of economic business via the Internet, which requires the creation of a trusted environment where customers can feel confident when making purchases, where the data of millions of people are shared, especially during online transactions, as this includes information Sensitive such as credit card numbers, personal identification numbers and login credentials, which must be secure, which calls for the need to implement cybersecurity. The close interrelationship between electronic commerce and cybersecurity; This is evident in cyber attacks. Where credit card data can be stolen from e-commerce sites. Not to mention undermining business and consumer confidence in that kind of trade.

The importance of the topic is that there is a strong relationship between cybersecurity and electronic commerce, as the decline in the effectiveness of cybersecurity increases the cost incurred to the point of undermining the confidence of consumers and companies in digital commerce. Hence, protection measures require international cooperation between the public and private sectors, since networks, institutions, and global supply chains rely on the same systems and programs that companies mostly provide, which means that there are shared risks.

Keywords: cyber security, electronic contract, electronic commerce, international law, cyber crime.

مقدمة :

تعتبر الجرائم السبرانية جرائم حديثة ،تبذل بشأنها مكافحات و جهود عظمى دولية و وطنية ، بحيث أن لها الأثر الكبير على المصلحة الاقتصادية و الاجتماعية و السياسية للدول ،وعليه ركز المجتمع الدولي البحث و وضع اتفاقيات و معاهدات دولية و قوانين وطنية ،لاسيما ما حدث في العالم جراء وباء كورونا جعل من حجم التعاملات الإلكترونية تكثر و يعود تطور التقنيات وتنامي استعمال الحاسوب والإنترنت وانتشار ثقافة المعلوماتية لدى الجمهور، عند بداية الثمانينيات من القرن العشرين الذي بدأ باستعمال الحاسوب من قبل القطاع الخاص، إلا أن استعماله في المعاملات اقتصر على إدخال البيانات واستخراجها وطباعة المستندات آلياً مما شكل نقلة نوعية عن الطباعة على الآلة الكاتبة أو عن حفظ الملفات ورقياً وبواسطة أنظمة أرشفة تقليدية . أدى السماح للجمهور باستعمال شبكة الإنترنت في بدايات التسعينيات من القرن الماضي، إلى ظهور أنواع جديدة من إمكانيات الاتصال والتعامل والتعاقد، وقد أدى بالتالي إلى إمكانية تبادل المعلومات في بداية الأمر ثم إلى تبادل الرسائل والمعاملات في وقت لاحق واستعمل كوسيلة لتسليم بعض المنتجات ذات الطابع الإلكتروني، وهو ما أصبح يعرف بالمعاملات الإلكترونية،

هذا ويمكن للنهج المشترك أن يُعزز الأمن السيبراني، ويحمي التجارة الرقمية، والعكس صحيح، فقد تسفر المعايير الأحادية عن الإفراط في حماية الأمن القومي، وانتهاك التزامات منظمة التجارة العالمية، واتفاقيات التجارة الحرة.

و لعل أحسن مثال هو ا فيروس الفدية WannaCry -الذي ينسب إلى كوريا الشمالية- الذي تسبب في إصابة أكثر من 200 ألف جهاز كمبيوتر في 153 دولة، وخسائر قدرت بملايين الدولارات. حيث أهمية الأمن السيبراني دفعت الكثير عددًا من الدول إلى التعاون الدولي، إذ يشير أحد التقديرات إلى تبني 50 دولة على الأقل سياسات ولوائح الأمن السيبراني، كما أكد الاتحاد الأوروبي ضرورة التعاون العالمي الوثيق لتبنى نهجٍ عالميٍ مشترك تجاه قضايا أمن الشبكات والمعلومات. كما أكدت استراتيجيةُ الأمن السيبراني الأمريكية الحاجةَ إلى تعزيز قدرة الحلفاء والشركاء في مواجهة التهديدات المشتركة.

تعتبر التجارة الإلكترونية بعدًا مزدهرًا للنمو الاقتصادي الحديث والتنمية ، حيث توفر العديد من الوظائف في جميع أنحاء العالم. و الأمن السيبراني يساعد على تعزيز وضمان الأسواق على التطور بشكل أفضل وأقوى وأكثر استدامة لكن في المقابل هذا الربط بينهما يثير مجموعة معقدة من القضايا؛فتنامي الشركات والحكومات والأفراد على التكنولوجيا. الرقمية ومن ناحية أخرى، لا بد من الاهتمام بظاهرة تقييد التدفق الحر للبيانات من قبل الحكومات، لما لها من عواقب وخيمة على التجارة الرقمية. ومن ناحية ثالثة، قد تقوض سياسات الأمن السيبراني الثقة في الاقتصاد الرقمي. ولذا، تتزايد أهمية القواعد التجارية الجديدة التي يمكنها تعزيز الأمن السيبراني، وتقليل الحواجز التجارية في الوقت عين،فالاشكالية المطروحة هنا :كيف للأمن السيبراني أن يكون وسيلة حمائية للتعاملات التجارية الاكترونية ؟

لمعالجة هذه الاشكالية قمنا بوضع الخطة الاتية:

المحور الأول: تحديات الامن السبراني على صعيد التجارة الالكترونية الدولية

المحور الثاني: تحديات الامن السبراني علي صعيد التجارة الالكترونية الداخلية

المحور الأول: تحديات الامن السبراني على صعيد التجارة الالكترونية الدولية

تمثل المبيعات الإلكترونية 14% من إجمالي المبيعات في العالم، وتستمر التجارة الإلكترونية بالنمو بمعدل سريع على الرغم من عدم الاستقرار الاقتصادي العالمي.

وبحسب تقرير نشره موقع"EcommerceGuide" ، من المتوقع استمرار هذه الأرقام بالازدياد لتصل إلى 22% في عام 2023. وبحسب إحصائيات التجارة الإلكترونية العامة بالنسبة لـ99 شركة لعام 2020، من المتوقع أن تجرى 95% من عمليات الشراء إلكترونيًا بحلول عام 2040، إذ تصدرت منطقة آسيا والمحيط الهادئ وأمريكا الشمالية التجارة الإلكترونية ومبيعاتها، وتليها أوروبا الغربية.

واكتسبت منطقة آسيا والمحيط الهادئ زيادة في التجارة الإلكترونية بمعدل 62%، بحسب تقرير أعده موقع"BusinessInsider" ، في 30 من كانون الأول 2020.

وبشكل عام، من المتوقع أن تجلب مبيعات التجارة الإلكترونية لعام 2021 ثلاثة تريليونات دولار، وأثّر نمو بعض المناطق بالتجارة الإلكترونية على تجارة التجزئة العالمية في عام 2020، إذ عُدلت تقديرات التجارة بالتجزئة بعد انتشار فيروس "كورونا المستجد" (كوفيد- 19) في العالم بنسبة 16.5.%، وشهدت منصات إلكترونية رائدة، مثل "أمازون"، ارتفاعًا طفيفًا في مبيعات التجارة الإلكترونية في أثناء تفشي جائحة "كورونا."

وزادت المبيعات عبر الإنترنت على عام 2019 بنسبة 15% في عام 2020، وأنفق المستهلكون حول العالم رقمًا قياسيًا بالشراء عبر الإنترنت قدره 10.8 مليار دولار، إذ ابتعد الناس عن المتاجر خوفًا من العدوى بالفيروس، واختاروا الخدمات الإلكترونية، بحسب موقع[364]."DigitalCommerce360"

يعرف الامن السبراني بأنه "النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار إلى خسائر دائمة."

أولا :قانون الاونسيترال النموذجي

1:بشأن التجارة الالكترونية 1996

يعتبر القانون النموذجي، القانون الذي يهدف الى ممارسة التجارة الكترونيا بمعنى باستعمال الوسائل الالكترونية و كان هو أول قانون يحتذى به دوليا من خلاله تم الاقتباس منه في التشريعات الوطنية ،فالقواعد التي أتى بها تهدف الى تذليل العقبات القانونية و حتى أنه جاءت في طياته التنبؤات عن التطورات القانونية

[364] https://www.enabbaladi.net/archives/444744#ixzz70nbjWA9c

فيما يخص مجال التجارة الالكترونية تعاقديا و جعل الامر متساوي بين التعاقد ورقيا و التعاقد الكترونيا ،ما يعزز من التجارة الدولية و يبسطها.

حيث أنه اعتمد على المبادئ التي تعتبر أسس التجارة الالكترونية الحديثة، و التي تخص الحياد التكنولوجي و التكافؤ الوظيفي، وأن هذا القانون كفل مبدا أساسي و هو مبدأ التكافؤ أو ما يسمى بعدم التمييز لأاي اثر قانوني لأي وثيقة الكترونية ،أما مبدأ الحياد التكنولوجي فيلزم باعتماد أحكام محايدة بشأن التكنولوجيا المستخدمة، ويحدّد مبدأ التكافؤ الوظيفي معايير يمكن بموجبها اعتبار الخطابات الإلكترونية مكافئة للخطابات الورقية[365]. فهو يبين الشروط التي يجب أن تستوفيها الخطابات الالكترونية.

كما أننا نجد في هذا القانون القواعد التي تحدد ابرام العقود بالوسائل الالكترونية و طرق إسنادها و الاقرار باستلامها و طرق إثباتها من مكان الارسال و التلقي أيضا[366]. .

2:القانون الاونسيترال النموذجي بشأن التوقيع الالكتروني 2001

أو ما يسمى بقانون التوقيعات ،ظهر بغرض توضيح ما شاب التصرفات التجارية الالكترونية من تساؤلات و منازعات فيما يخص التوقيع الالكتروني ، فهناك من عرف التوقيع الالكتروني بانه ذلك التوقيع الناتج عن اتباع اجراءات محددة تؤدي في النهاية الى نتيجة معينة معروفة مقدما و يكون مجموع هته الاجراءات هو البديل الحديث للتوقيع التقليدي او ما يسميه البعض التوقيع الاجرائي[367] .

و يعرفه فقه القانون الفرنسي بانه مجموعة من الاجراءات التقنية التي تسمح بتحديد من تصدر منه هذه الاجراءات و قبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته[368] . وعليه نجد في هذا القانون النموذجي مواد تبين كيفية استخدام التوقيعات الالكترونية و تيسير استخدامها

---

[365] قد أصبح هذا النوع من الصكوك ضروريا بسبب النمو الكبير الذي تشهده العمليات التجارية التي تنطوي على استعمال التكنولوجيا العصرية و انتشار استخدام الخطابات الالكترونية في العقود الدولية.

[366] قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية (1996)الموقع الالكتروني للامم المتحدة باللغة العربية ، https://uncitral.un.org شوهد ،تاريخ 2021/05/16. بتوقيت16.00.

[367] د: خالد مصطفى فهمي، النظام القانوني لتوقيع الإلكتروني في ضوء التشريعات العربية والاتفاقات الدولية ،دار الجامعة الجديدة، اسكندرية، 2007 ،ص 44،45.

[368] د.ايمن سعد سليم ، التوقيع الالكتروني دراسة مقارنة ، دار انهضة العربية،القاهرة ، 2004 ،ص27.

حيث أنه وضع معايير يتم اتباعها فيما يخص التوقيعات الالكترونية و وضع قوة ثبوتية لها تعادل قوة ثبوتية التوقيع الخطي ،الامر الذي ساعد الدول بوضع قوانين للتوقيعات الالكترونية و يعزز من قوة ثبوتية هذا التوقيع

كما اننا نجد أن قواعده موافقة لما جاء به قانون التجارة الالكترونية النموذجي و هو مبدا الحياد التكنولوجي و نص أيضا على كل من حقوق وواجبات المتعاقدين الموقعين و حت على الغير الذي يتدخل في عملية التوقيع.

و نجد أن المشرع الجزائري قد عرفه و نظمه ضمن القانون الخاص بالمواصلات السلكية و اللاسلكية حيث نص في المرسوم التنفيذي رقم 123-01 المتعلق بالخدمات المواصلات السلكية واللاسلكية المعدل و المتمم بالمرسوم التنفيذي رقم 162-07 حيث نجد المادة 03 مكرر01 الخاصة بالتعريف التوقيع الالكتروني تنص على انه معطى ينجم على استخدام اسلوب عمل يستجيب للشروط المحددة في المادتين 323مكرر و323 مكرر01 من الامر رقم 75 /58 المؤرخ في 26 سبتمبر و ينص على نوع ثاني من التوقيع الالكتروني المسمى بالتوقيع الالكتروني المؤمن في الفقرة الثانية من نفس المادة و هو ذلك التوقيع الذي يفي بالمتطلبات الاتية ،يكون خاصا بالموقع و يتم انشاؤه بالوسائل يمكن الاحتفاظ بها تحت رقابته الحصرية ،يكون قابلا للكشف عن أي تعديل يلحق بالفعل المرتبط به .

ثانيا : اتفاقية الأمم المتحدة بشأن استخدام الخطابات الإلكترونية في العقود الدولية (نيويورك، 2005)

ان الهدف من وضع هذه الاتفاقية هو تسهيل استخدام الخطابات الالكترونية في مجال التجارة الدولي و ذلك بشرط التأكد من صحة ابرام العقود و غيرها من الخطابات الالكترونية في نفس صحة العقود الورقية، فاتفاقية الخطابات الإلكترونية هي عبارة عن معاهدة تمكينية يتمثل أثرها في تذليل تلك العقبات الرسمية من خلال تحقيق التكافؤ بين شكلي الخطابات الإلكتروني والمكتوب.

وأيضا ما جاء في هذه الاتفاقية هو تذليل المنازعات الحاصلة في هذا المجال و يسهل استخدامها فالقصد من الاتفاقية هو تعزيز القواعد المتعلقة بالتجارة الإلكترونية و التوحيد في اشتراع قوانين الأونسيترال النموذجية على الصعيد الوطني فيما يتعلق بالتجارة الإلكترونية، وكذلك تحديث واستكمال بعض أحكام تلك القوانين النموذجية في ضوء الممارسات الأخيرة. ووضع قواعد موحدة دوليا .

ان القواعد التي اتت بها هذه الاتفاقية أساسا جاء بها قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية وقانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية..

وتنطبق الاتفاقية على جميع الخطابات الإلكترونية المتبادلة بين طرفين يقع مقرا عملهما في دولتين مختلفتين، على أن يكون مقر عمل أحدهما على الأقل موجودا في دولة متعاقدة ما جاءت به المادة الاولى. ويمكن أيضا تطبيق الاتفاقية باختيار الطرفين. وتُستبعد من نطاق انطباق الاتفاقية العقود المبرمة لأغراض شخصية أو عائلية أو منزلية، كالمتعلق منها بقانون الأسرة وقانون الخلافة، وكذلك بعض المعاملات المالية، والصكوك القابلة للتداول، ومستندات الملكية وهذا ما جاء في نص المادة الثانية ..

كما انا نجد في نص المادة 09 أنه يوجد تكافؤ بين العقد الورقي والعقد الالكتروني و ايضا فيما يخص قوة الاثبات، وفضلا عن ذلك، فإن الاتفاقية تنص على المبدأ العام القائل بعدم جواز إنكار صحة الخطاب من الناحية القانونية لمجرد كونه في شكل إلكتروني (المادة 8). ونظرا لانتشار نظم الرسائل الآلية على وجه التحديد، فإن الاتفاقية تتيح إمكانية إنفاذ العقود المُبرمة بواسطة هذه النظم، و ما جاءت به المادة 03 فان هذه الاتفاقية تجيز للأطراف التعاقدية استبعاد تطبيق هذه الاتفاقية أو تغيير شروطها ضمن الحدود التي تسمح بها الأحكام التشريعية المعمول بها في خلاف هذه الحالة

-ثالثا: اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكررية :

تم التوقيع عليها من قبل الدول الاعضاء لسنة 1994،تم فيها ذكر و دراسة التعريفات لمصطلحات التجارة و حقوق الملكية الفكرية و تضمنت العديد من الاجراءات المهمة و الفعالة لردع الاعتداء على حقوق الملكية اللفكرية ،و أيضا تفرض على الدول اتخاذ العديد من التدابير المهمة لمعالجة الوضع .

رابعا : جهود منظمة الامم المتحدة في ميدان حماية الحياة الخاصة ،

و ذلك في مواجهة التقدم الالكتروني و حماية حياة الافراد و حرياتهم من خطر التعدي عليها في المؤتمر الدولي الاول لحقوق الانسان الخاص بأثر التقدم التكنولوجي على حقوق الانسان في مؤتمر طهران 1968.

و جاء في توصياته أن الحاسبات الالكترونية تمثل اكبر تهديد للحياة الخاصة بالحرية الشخصية على الحاسب الالي و تحليلها مما يكشف على أنماط التعامل و العلاقات[369].

[369] **علي جبار الحسناوي ،جرائم الحاسوب و الانترنت ،دار اليازوري ،للنشر والتوزيع،2009،الاردن ،ص149.**

المحور الاول :تحديات الامن السبراني علي صعيد التجارة الالكترونية الداخلية .

ان مكافحة جرائم الانترنت على المستوى الوطني تقتضي توثيق روح التعاون بين الانظمة القانونية الداخلية و تظهر معالم هذا التقارب في قبول حالات تفويض الاختصاص ،و في اتخاذ اجراءات التحقيق و جمع الادلة و تسليم المجرمين و الاعتراف بالاحكام الجنائية،سنتطرق الى قانون التجارة الالكتروني الجزائري و قانون الاجراءات الجزائية و قانون العقوبات

أولا :القانون 18-05

إن المستهلك عبر الإنترنت ليس مجرد متسوق ولكنه أيضًا مستخدم لتقنية المعلومات[370] ،فقد أصبح يطلق على المستهلك أو المشتري الذي يمارس عمليات الشراء عبر شبكة الأنترنت بالمشتري عبر الأنترنت، فهو يختلف في صفاته وخصائصه وطبيعة طلباته عن (المستهلك/المشتري) العادي، ويتوقع من البائعين على شبكة الانترنت خدمات أفضل بكثير مما هو سائد في عمليات البيع التقليدية، كما يتوقع أيضا أسعارا أقل ونظم تسليم أسرع وأفضل مع توفير جميع البيانات والمعلومات ذات العلاقة بالمنتج (سلعة أو خدمة)..، ويتوقع أيضا أن تمر أساليب دفع أثمان المنتجات في قنوات آمنة مع القضاء على عمليات الاختراق الالكتروني التي تتسبب في السرقات من حسابات المشترين، فقد باتت مسالة أمن البينات والمعلومات عبر الشبكة العالمية هي جوهر القضايا المهمة التي يضعها المشتري عبر الانترنت ضمن الأولويات الأولى عند التسوق الالكتروني[371].

افرز معه توجه المستهلك نحو المواقع التجارية الالكترونية لتعدد الخدمات المعروضة مع المزايا المتعددة في العرض و الاسعار فأهمية الخدمات الالكترونية على شبكة الانترنت زادت من اقبال المستهلكين على هذه الخدمات و جعلت منها محور طلب للكثير منهم ،فيما يخص الحماية الجنائية فهناك اربعة جرائم شايعة فيما يخص المعاملات الالكترونية التجارية و هي : جريمة السرقة في مجال المعاملات الالكترونية ،جريمة الاحتيال ،جريمة خيانة الامانة و جريمة التزوير.

ثانيا :طرق تسوية منازعات عقود التجارة الدولية الالكترونية، وحماية الطرف المتضرر

ان تعدد المعاملات المبرمة الكترونيا أدت الى تكوين مجال خصب للمنازعات تنشأ بين الاطراف المتعاقدة ،ونظرا لطابعها الدولي ادى الى البحث عن ما هو القانون الواجب التطبيق . نظرا لارتباط العلاقة القانونية بأكثر

---

[370] **Efthymios Constantinides, nfluencing the onlineconsumer's behavior:the Web experience, Internet Research, Volume 14 · Number 2, Emerald Group Publishing Limited,UK, 2004, p111.**

[371] **يوسف أحمد أبو فارة، التسويق الالكتروني- عناصر المزيج التسويقي عبر الأنترنت، الطبعة الثالثة، دار وائل للنشر والتوزيع، عمان، الأردن، 2009، ص416.**

من نظام قانوني واحد ، تحيلنا مثل هذه العلاقة إلى قواعد القانون الدولي الخاص ومبدأ تنازع القوانين لتحديد القانون الواجب التطبيق من بين القوانين المتصلة بالعقد. وإن كان مبدئيا وكما أشارت إليه أغلب القوانين الوطنية والدولية هو تطبيق قانون الإرادة وبالتالي فالقانون الواجب التطبيق ،هو القانون الذي اختاره الأطراف صراحة أو ضمنيا[372]،

لكن مجال التنازعات هو مجال معقد ليس بهذه السهولة ففي الكثير من الاحيان لا يتم تحديد القانون الواجب التطبيق مسبقا ، الأمر الذي يطرح مسالة تنازع القوانين لدول الأطراف المتعاقدة ،و أيضا مسألة تحديد المحكمة المختصة و هذه الامور كلها تمتاز بالتعقيد ،فتعتبر فكرة تنازع القوانين النتيجة الحتمية للتزاحم في ماهو القانون الواجب التطبيق و عليه تتم عملية الخيار أو المفاضلة بين القوانين الانسب في حل المنازعة العقدية بين الأطراف، فالقانون الدولي الخاص أعد لمهمة حل مسألة تعدد الأنظمة القانونية التي تحكم علاقة قانونية واحدة عن طريق نظرية تنازع القوانين المعتمدة أصلا على قواعد قانونية محايدة تسمى بقواعد الإسناد التي تحدد القانون المطبق على العلاقة المتضمنة لعنصر أجنبي، وذلك بالارتكاز على ضوابط تكون في أغلب الأحيان مكانية، أي في إقليم جغرافي محدد، مما يتنافى مع طبيعة عقود التجارة الإلكترونية التي تبرم عبر شبكة مفتوحة على العالم[373].

1-حماية المتضرر في عقود التجارة الالكترونية من قاعدة الاسناد الشخصي[374] :

ما يسمى بمبدأ سلطان الارادة في اختيار القانون الواجب التطبيق في حالة حدوث منازعة ،و يجب توفر شروط لوضع هذه الارادة تتمثل في

أ- وجوب ارتباط القانون بعلاقة حقيقية بالأطراف أو المعاملات التجارية، وأن يطفى المنطق على اختيار الأطراف .

---

[372] هشام علي صادق، القانون الواجب التطبيق على عقود التجارة الدولية، منشأة المعارف، الإسكندرية، 1995 ، ص 61.

[373] خليفي سمير ،حل النزاعات في عقود التجارة الالكترونية مذكرة ماجستير في القانون الدولي ،جامعة مولود معمري تيزي-وزو2010/10/28 ص17.

[374] المادة 01/301 من القانون التجاري الموحد للولايات المتحدة الأمريكية، على أن ": الأطراف في المعاملات الدولية يجوز لهم الاتفا ق وفقا لقانون أية ولاية أو دولة أخرى، سواء كانت هذه المعاملة ذات صلة بهذه الدولة أو الولاية أم لا"، وتضيف الفقرة 2 من نفس المادة على أن: "الأطراف في المعاملات الدولية أيا كانت حقوقهم والتزاماتهم لهم الحرية الأساسية في اختيار القانون الواجب التطبيق على عقودهم، سواء كانت المعاملة ذات صلة بالدولة أو الولاية المعنية،إبراهيم أحمد سعيد زمزمي، القانون الواجب التطبيق في منازعات عقود التجارة الالكترونية، دراسة مقارنة، رسالة للحصول على درجة الدكتوراه، جامعة عين الشمس، كلية الحقوق، قسم الدراسات العليا، مصر، 2006 ، ص 96.

ب- أن لا يتعارض القانون المختار مع أية سياسة جوهرية لدولة القاضي أو الدولة التي سوف يكون قانونها هو الواجب التطبيق على العقد[375].

وهذا ما أكدته جل الاتفاقات الدولية نذكر منها ،الاتفاقية الأوربية الخاصة بالتحكيم التجاري الدولي المبرمة في جنيف في 12أفريل 1961 ودخلت حيز التنفيذ في سبتمبر 1964 ،في المادة 7 منها على أن "الأطراف أحرار في تحديد القانون الواجب التطبيق على النزاع "...، بالإضافة إلى اتفاقية واشنطن المنشأة للمركز الدولي لفض منازعات الاستثمار بين الدول ورعايا الدول الأخرى، فتنص المادة 42 من الاتفاقية "" : تفصل المحكمة في النزاع طبقا للقواعد التي يقررها الأطراف[376]) ".

و ايضا اتفاقية مكسيكو لعام 1994 المبرمة بين دول الاتحاد الأمريكي، والخاصة بالقانون الواجب التطبيق على العقود الدولية، في المادة 7على أن ": العقد يخضع لأحكام القانون الذي اختاره الأطراف، وأن اختيار الأطراف على هذا الاختيار يجب أن يكون واضحا وجليا، وفي حالة عدم وضوح هذا الاتفاق يستخلص ضمنيا من سلوك الأطراف ومن بنود العقد[377]"

وايضا الهيئة الدولية لتوحيد القانون الخاص UNIDROIT أعطت للأطراف الحق في إبرام العقد وتحديد مضمونه، كما أقرت الاتفاقيات وقوانين ولوائح التحكيم على قانون الإرادة، فمنها لجنة الأمم المتحدة لقانون التجارة الدولية التي سنّت قواعد التحكيم CNUDC،فتنص المادة 1/33 منها على أن "": تطبق هيئة التحكيم على موضوع النزاع القانون الذي عينه الأطراف[378].

2-اشكاليات تطبيق هذا المبدأ :

تبرم العقود الإلكترونية التجارية على العموم بين مورد للسلع أو الخدمات من جهة، ومستهلك من جهة ثانية، و يكون المستهلك هو الطرف المتضرر في الكثير من الاحيان لذلك سعت القوانين لحمايته حيث أنه

---

[375] Julien le claiche, La détermination de la loi et le juge compétent, disponible sur le site – www.droit-ntic.com p 06.

[376] خالد ممدوح إبراهيم، التحكيم الإلكتروني في عقود التجارة الدولية، دار الفكر الجامعي للنشر، الإسكندرية، 301 .ص، 2008 و -قبايلي الطيب، نظام تسوية المنازعات في إطار المركز الدولي لفض منازعات الاستثمار بين الدول ورعايا الدول الأخرى CRDI ،مذكرة لنيل درجة الماجستير، فرع قانون الأعمال، جامعة مولود معمري، 2001/2000 ،ص 9 .

[377] - VERBIEST Thibault, Commerce électronique : loi applicable et juridiction compétente, sur le site : www.journaldunet.com. p. 03.

[378] CHATILLON Stéphane, Le contrat international, 3ème édition, Vuibert, Paris, 2007, p.268.

يكون غير قادر على رؤية المنتج في أغلب الأحيان، أو التأكد من طبيعة الخدمة الموقعة قبل توقيع العقد، عمل التوجيه الأوربي رقم EEC ،وذهب أيضا التوجيه رقم EC/ 7/97 الخاص بحماية المستهلكين فيما يتعلق بالعقود عن بعد ، ففي حالة اختيار المنتج لقانون معين لكي يحكم النزاع، فإن المستهلك لن يكون أمامه سوى الدفع بعدم شرعية شروط المنتج في اختيار قانون ما لحكم النزاع، ودعم حماية المستهلك الفقرة الأولى من ملحق التوجيه الأوربي لعام 1993 ،الذي اعتبر إلزام المستهلك ببنود أدرج فيها شرط تعسفي، يجيز له المطالبة بعدم تطبيق القانون المتفق عليه.

أكدت كذلك اتفاقية روما لعام 1980 المتعلقة بالالتزامات التعاقدية في المادة 2/5 منها على أن قانون الإرادة يمكن استبعاده إذا كان من شأنه أن يحرم المستهلك من الحماية التي يوفرها قانون الدولة التي بها محل إقامته العادية، وهذا ما يجعل من قانون الإرادة كأنه مركز خطورة في العملية التعاقدية[379].

تلجأ إرادة الأطراف في بعض الحالات إلى تجزئة العقد واختيار أكثر من قانون لحكم الرابطة العقدية، كالاعتماد على قانون يقبل التوقيع الإلكتروني ويقر بصحة المستندات المحررة عن طريق شاشات الحواسب الآلية، ويثبت صفتها بأنها محررات رسمية يقبل الإثبات بها، وقانون لا يقبل بمثل هذه المعاملات ولا يقرر برسميتها، مما يحدث تباعد بين قانونين متضاربين اختارهما الأطراف للتطبيق على واقعة قانونية ما يجعل من مبدا قانون الارادة غير ملائم و غير صالح للتطبيق على النزاعات المترتبة عن عقود التجارة الإلكترونية، من دون أن ننسى ان ميدان التجارة الالكترونية فرضت على المبدأ العديد من الحدود الملزمة للتطبيق على مثل هذه العقود

كما أن تدخل القاضي في تحديد القانون الواجب التطبيق في النزاع يعتبر حماية للطرف الضعيف في العلاقة، ما أخذ به القانون المدني الجزائري بعد التعديل الأخير 10/05 فحسب المادة 18 التي اشترطت وجود صلة حقيقية بين العقد والقانون المختار .

تقيد إرادة المتعاقدين في اختيار القانون الذي يطبق على عقود التجارة الإلكتروني ة من أجل عدم إطلاق الحرية الكاملة للأطراف، فلا بد أن تكون هناك رابطة حقيقية وجادة بين العقد والقانون المختار، فلا يمكن اختيار قانون أجنبي منعدم الصلة بالعقد، فيكون القانون المختار غير قانون أي من المتعاقدين ولا قانون مكان إبرام العقد أو تنفيذه .

---

[379] سمير خليفي ،حل المنازعات في عقود التجارة الالكترونية ،المرجع السابق صفحة 32.

حماية الطرف المتضرر من عيب الغش في القانون :

قد يلجأ المتعاقدين الى الاتفاق على وضع قانون دولة ما ارادوا تطبيق قانونها و ذلك للتحايل و تحقيق مصالح ماكان قانون دولتيهما أن يحققها لهما، فتلعب الإرادة فيها دورا جوهريا في تغيير ضابط الإسناد، والإفلات من تطبيق أحكام القانون الواجب التطبيق على العقد . تحديد أثر الدفع بالغش نحو القانون في حالة التأكد والتيقّن من توافر نية الغش، يعود إلى عدم الاعتداد بالتغيير الذي أجراه الأطراف، باعتبار أن القصد من التحايل هو الهروب من أحكام القانون المرتبط بالعلاقة التعاقدية، ومن ثم يكون الجزاء بتطبيق أحكام القانون المختص الذي سعت إرادة الأطراف إلى تجنبه باتفاقهم[380].

فكرة النظام العام و احترامه الية للحماية القانونية للطرف المتضرر :

يؤكد غالبية الفقهاء على أهمية النظام العام كأداة لاستبعاد القانون الأجنبي الذي تم اختياره من الأطراف للتطبيق على العقد، إذا تعارض مضمون هذا القانون مع الأسس الجوهرية في المجتمع ، وتتجلى فكرة النظام العام في مجال التجارة الإلكترونية من خلال النصوص التي تحظر ممارسة الأنشطة غير المشروعة في هذا المجال، وكمثال المقدم من طرف الأستاذ HUET فيما يخص تحديد السعر في البورصة، حيث يتم تنظيمه بشكل دقيق ويمنع نشره على شبكة الإنترنت .يجب أن يكون اختيار القانون الواجب التطبيق لدولة معينة، لا يمس بأية حال النظام العام الساري في الدولة الأجنبية التي تم اختيار قانونها لحكم العلاقة التعاقدية، وإلا فالقاضي يقوم بجهل القانون المختار ليعين القانون الأقرب للعلاقة القانونية محل النزاع، ومن بين الاتفاقيات الدولية التي أخذت بهذه الفكرة نجد اتفاقية لاهاي عام 1955 التي نصت على استبعاد القانون المنصوص عليه في الاتفاقية إذا كان يمس بالنظام العام [381].

3-الوساطة الالكترونية :

تعرف الوساطة الإلكترونية بأنها من أهم الوسائل البديلة لحل النزاعات الناشئة عن العقود المبرمة بالوسائل الإلكترون ةي ، وذلك باستعانة أطراف النزاع بوسيط يعمل على تقديم النصح والإرشاد وربط الاتصال بين الأطراف، كما يطرح بعض الاحتمالات وللأطراف الحرية التامة في قبولها دون ضغط أو إكراه لحل النزاع

---

[380] ونصت المادة 24 من القانون المدني الجزائري على أن:" لا يجوز تطبيق القانون الأجنبي بموجب النصوص السابقة إذا كان مخالفا للنظام العام، أو الآداب في الجزائر، أو أثبت له الاختصاص بواسطة الغش نحو القانون، فيطبق القانون الجزائري محل القانون الأجنبي المخالف للنظام العام أو الآداب العامة"، راجع نص المادة 24 من القانون رقم 05-10 المؤرخ في 20 يونيو 2005

[381] Selon L'article 06 de la convention de la Haye de 1986 : « L'application de la loi déterminée par la présente convention peut être écartée pour un motif d'ordre public », voir : - FROMENT Camille ,op.cit, p. 24

القائم بينهما، كما للأطراف مكنة العدول في كل لحظة عن السير قدما في هذا الطريق ليختاروا الطريق التقليدي في التقاضي .يعتبر الوسيط عامل محايد وتطوعي شرط موافقة الأطراف العمل معه للوصول إلى نتيجة عسى أن تكون حلا وسطا للنزاع[382].

ولقد عرفتها المادة 03/01 من قانون الأونيسترال النموذجي للتوفيق التجاري الدولي بأنها: " عملية يتم من خلالها حل النزاع وديا، سواء بالوساطة أو التوفيق، مع محاولة الوسيط الوصول لحل ودي للنزاع العقدي أو القانوني دون أن يملك سلطة إجبار المتنازعين على قبول الحل "، ويتم الإشراف على العملية مراكز الوساطة الإلكترونية التي تمنح كل الوسائل المادية والبشرية لإنجاح العملية قصد الوصول إلى حل يرضي الطرفين، وتضع تحت تصرفهم المواقع الإلكترونية التابعة للمركز قصد حسن سير العملية[383].

4-التوفيق الالكتروني :

وهو يشبه تقريبا الوساطة الالكترونية ،عرفته المادة 1/3من قانون الأ يسنو ترال النموذجي للتوفيق التجاري الدولي أنه: " أي عملية سواء أشير إليها بتعبير التوفيق أو المصالحة أو الوساطة، وهو الطلب المقدم من الطرفين إلى شخص أو عدة أشخاص آخرين قصد مساعدتهما في سعيهما إلى التوصل لتسوية ودية لنزاعهما الناشئ عن علاقة تعاقدية أو قانونية مهما كان نوعها، وعلاقة متصلة بالعقد، ولا يكون للموفق أية صلاحية في فرض حل للنزاع على الطرفين"، ليبقى التوفيق أنه محاولة لتقريب وجها النظر بين الطرفين المتنازعين قصد الوصول إلى حل يرضي الطرفين [384].

5-التحكيم الالكتروني :

فآلية التحكيم وطالما أصبح أسلوبا حضاريا ومتقدما لتسوية النزاعات، واللجوء إليه أصبح اليوم ظاهرة عالمية نظرا لما يتيحه من خيارات نوعية التحكيم وحتى المحكمين وكذا القانون الواجب التطبيق .وجد المتعاملون في مجال التجارة الإلكترونية غايتهم في التحكيم التجاري الإلكتروني ، والذي لا يقف عند حد تسوية المنازعات الإلكترونية فقط، بل يمكن اللجوء لتسوية المنازعات التجارية العادية، مثل: عقود الاستهلاك، التأمين، الملكية

---

[382] **إبراهيم أحمد سعيد زمزمي، المرجع السابق، ص 227.**

[383] **I. Verougstraete, Le Juge et La Médiation, revue de la cour suprême, numéro spécial, Mode Alternatifs de Règlement des litiges : Médiation, conciliation et Arbitrage, le 15-16 juin 2008, Tome 2, Alger, 2008, p.54.**

[384] **قانون الأونسيترال النموذجي للتوفيق التجاري الدولي مع دليل اشتراعه واستعماله، منشورات الأمم المتحدة، بناء على قرار الجمعية العامة رقم 57/562 ،المؤرخ في 2000/11/19.**

الفكرية، بما يحقق مزايا تتشابه مع التجارة الإلكترونية من توفير النفقات والانجاز السريع للتسوية)وتوفير الوقت الذي له بالغ التأثير في المعاملات التجارية[385].

قانون العقوبات المعدل و المتمم بالقانون 04-05 المؤرخ في 2004 المساس بأنظمة المعالجة الالية للمعطيات و ذلك في المواد 394 مكرر الى 394 مكرر7.

أ-جريمة الدخول أو البقاء غير المشروع :

ان عقوبة الدخول أو البقاء داخل نظام المعالجة الالية للمعطيات لا يتطلبان حدوث نتيجة معينة كالوصول الى المعطيات و البرامج و التلاعب بها فإذا لم ينجم عن الدخول او البقاء الغير المشروع الغير المصرح به بهما اعاقة او افساد للنظام المعالجة الالية او ازالة او تعديل لمعطيات التي يحتويها النظام و اما عدم صلاحية النظام لاداء وظائفه هي الحبس من ثلاث أشهر الى سنة و الغرامة من 50000 الى 100000 دج ، و اذا تم التعديل او ازالة فانه ترتفع العقوبة الى ضعف عقوبة الدخول فقط .

من ثلاث اشهر الى ستة اشهر الى من سنة الى سنتين و الغرامة 100.000دج الى 200000 دج.

ب- جريمة التلاعب بمعطيات الحاسب الالي :المادة 394 مكرر1 هي الحبس من ستة أشهر الى ثلاث سنوات و غرامة 500.000 دجالى 2000.000 دج.

ت- جريمة التعامل في معطيات غير مشروعة المادة 394 مكرر2 قانون عقوبات هي الحبس من شهرين الى ثلاث سنوات و غرامة من 1000.000 دج الى 5000.000 دج.

وعقوبات تكميلية تشترك فيها مع سائر جرائم المعطيات و تتعلق هذه الجرائم في العقاب على الاتفاق الجنائي المجسد بأعمال مادية او العقاب على الشروع.

الخاتمة :

لقد نتج على التغييرات التي احدثتها نظم المعلومات في مجال الجريمة عدة مشكلات فيما يخص التجارة الالكترونية الامر الذي أدى بالمجتمع الدولي الى وضع النقاط على الحروف كون أن التجارة الالكترونية هي اساس الاقتصاد الدولي اليوم.

[385] حابت آمال، التحكيم عبر الإنترنت، الملتقى الدولي، " التحكيم التجاري الدولي بين التكريس التشريعي والممارسة التحكيمي، بجاية أيام 14-15 جوان 2006 ،الجزء الأول، ص 255.

ان السياسة الجنائية هدفها الحد من الجرائم السبرانية بواسطة نظام عقابي ملائم و قانون اجرائي يوفر الضوابط

استحدث المشرع الجزائري نصوصا قانونية خاصة بالقواعد الاجرائية قصد مكافحة الجرائم المعلوماتية سواءا في قانون الاجراءات الجزائية أو قانون الخاص بالرقابة من الجرائم المتصلة بالتكنولوجيا الاعلام و الاتصال و مكافحتها،فيجب ان تكون الاتفاقات الدولية تراعي خصوصية القوانين الدولية ايضا و على القوانين الداخلية ايضا يجب ان تتوفر على شرط التطابق مع الاتفاقات الدولية

وعليه من هذه الورقة البحثية نستنتج مايلي :

- ان المكافحة الدولية للجريمة السبرانية فيما يخص موضوع التجارة الالكترونية قاصرة جدا
- غياب سياسات وطنية تواجه مخاطر جرائم الانترنت التي تستهدف التجارة الالكترونية .

التوصيات :

1-ضرورة تخصيص غرف في المحاكم بالجريممة السبرانية و تكوين قضاة مختصين في الامن السبراني

2-ضرورة تعزيز الامن الرقمي التجاري في الدولة عن طريق استعمال الذكاء الاصطناعي و ادخال تطبيق الهوية الرقميةpass-app

3-ضرورة تسهيل عملية التبليغ و السرعة في اجراء التحقيق و ذلك لطبيعة الجريمة السبرانية السريعة

4-وجوب تحسين الادوات التقنية في جمع الادلة في مجال التعاون الدولي.

قائمة المراجع :

- **القوانين :**

- القانون النموذجي الصادر عن الأمم المتحدة بشأن التجارة الإلكترونية، 01.لسنة 1996. در هذا القانون في 12 جوان 1996 عن لجنة الأمم المتحدة للقانون التجاري الدولي، وتم إقراره بناء على التوصية الصادرة عن الجمعية العامة للأمم المتحدة رقم - 51 662 في 16 ديسمبر 1996
- قانون التوجيه الأوروبي 97-7
- قانون التجارة الالكترونية 18-05 المتعلق بالتجارة الالكترونية المؤرخ في 24 شعبان 1439الموافق ل10 ماي 2018
- قانون الأونسيترال النموذجي للتوفيق التجاري الدولي مع دليل اشتراعه واستعماله، منشورات الأمم المتحدة، بناء على قرار الجمعية العامة رقم 57/562 ،المؤرخ في 2000/11/19.
- القانون المدني الجزائري القانون رقم 05-10 المؤرخ في 20 يونيو 2005

- **الكتب و الرسائل:**

- خالد مصطفى فهمي، النظام القانوني لتوقيع الإلكتروني في ضوء التشريعات العربية والاتفاقات الدولية ،دار الجامعة الجديدة، اسكندرية، 2007
- د.ايمن سعد سليم ، التوقيع الالكتروني دراسة مقارنة ، دار انهضة العربية،القاهرة ، 2004
- يوسف أحمد أبو فارة، التسويق الالكتروني- عناصر المزيج التسويقي عبر الأنترنت، الطبعة الثالثة، دار وائل للنشر والتوزيع، عمان، الأردن، 2009،
- هشام علي صادق، القانون الواجب التطبيق على عقود التجارة الدولية، منشأة المعارف، الإسكندرية، 1995
- خليفي سمير ،حل النزاعات في عقود التجارة الالكترونية مذكرة ماجستير في القانون الدولي ،جامعة مولود معمري تيزي-وزو2010/10/28
- إبراهيم أحمد سعيد زمزمي، القانون الواجب التطبيق في منازعات عقود التجارة الالكترونية، دراسة مقارنة، رسالة للحصول على درجة الدكتوراه، جامعة عين الشمس، كلية الحقوق، قسم الدراسات العليا، مصر، 2006
- خالد ممدوح إبراهيم، التحكيم الإلكتروني في عقود التجارة الدولية، دار الفكر الجامعي للنشر، الإسكندرية، 2008
- قبايلي الطيب، نظام تسوية المنازعات في إطار المركز الدولي لفض منازعات الاستثمار بين الدول ورعايا الدول الأخرى CRDI ،مذكرة لنيل درجة الماجستير، فرع قانون الأعمال، جامعة مولود معمري، 2001/2000
- حابت آمال، التحكيم عبر الإنترنت، الملتقى الدولي، " التحكيم التجاري الدولي بين التكريس التشريعي والممارسة التحكيمي، بجاية أيام 14-15 جوان 2006 ،الجزء الأول.

▪ **المراجع باللغة الاجنبية :**

-Julien le claiche, La détermination de la loi et le juge compétent, disponible sur le site – www.droit-ntic.com.

-VERBIEST Thibault, Commerce électronique : loi applicable et juridiction compétente, sur le site : www.journaldunet.com.

-CHATILLON Stéphane, Le contrat international, 3ème édition, Vuibert, Paris, 2007.

-Selon L'article 06 de la convention de la Haye de 1986 : « L'application de la loi déterminée par la présente convention peut être écartée pour un motif d'ordre public », voir : -FROMENT Camille .

-I. Verougstraete, Le Juge et La Médiation, revue de la cour suprême, numéro spécial, Mode Alternatifs de Règlement des litiges : Médiation, conciliation et Arbitrage, le 15-16 juin 2008, Tome 2, Alger, 2008.

-Efthymios Constantinides, nfluencing the onlineconsumer's behavior:the Web experience, Internet Research, Volume 14 · Number 2, Emerald Group Publishing Limited,UK, 2004.

الموقع الالكتروني: https://uncitral.un.org

استراتيجيات الأمن السيبراني في حماية التجارة الإلكترونية في القانون الموريتاني

عبد الله البشير
محام، عضو بالمكتب التنفيذي بمنظمة شباب المحامين العرب (موريتانيا)

ملخص باللغة العربية:

قدمت هذه الورقة علي هامش المؤتمر العلمي الدولي تحت عنوان : الأمن السيبراني في تشريعات الدول العربية المنعقد يومي الجمعة و السبت 16 و 17 يوليو 2021 بنادي المحامين تاركة مراكش- بالمملكة المغربية تحت عنوان : استراتيجيات الأمن السيبراني في حماية التجارة الإلكترونية في القانون الموريتاني.

و هي تتحدث بشكل مفصل عن الاستراتيجية الموريتانية لأمن السيبراني و عن قانون التجارة الإلكترونية الموريتاني المعروف بقانون المبادلات الإلكترونية .

ترجمة الملخص باللغة الانجليزية :

This paper was presented on the sidelines of the International Scientific Conference under the title: Cyber Security in the Legislation of Arab Countries, held on Friday and Saturday 16 and 17 July 2021 at the Lawyers Club, leaving Marrakesh - Kingdom of Morocco under the title: Cybersecurity Strategies in the Protection of E-Commerce in Mauritanian Law.

It talks in detail about the Mauritanian cyber security strategy and the Mauritanian e-commerce law known as the electronic exchanges law.

المقدمة

تعد استراتيجية الأمن السيبراني عنصرا مهما في استراتيجيات الأمن الوطني و الاجتماعي و الاقتصادي لأي بلد . إن التهديدات السيبرانية ذات طابع عالمي ، و لذلك فإن ضمان الأمن السيبراني له أهمية كبيرة علي المستويين الوطني و الدولي .[386]

و قد أصبحت الاستراتيجيات الوطنية للأمن السيبراني أكثر أهمية بالنسبة لأي بلد . و في هذا الإطار يلاحظ أن دول العالم تسير ببطء في عملية تطوير و تنفيذ استراتيجياتها للأمن السيبراني علي الرغم من التهديدات لأمنها و منها موريتانيا. و هذا ما أدركته الدولة الموريتانية حيث كانت سابقة في ذلك حيث وضعت استراتيجية لأمن السيبراني وسنتحدث عنها بالتفصيل من خلال هذه الورقة المتواضعة .[387] كما أننا سنسلط الضوء علي قانون حماية التجارة الإلكترونية الموريتاني المعروف بقانون المبادلات الإلكترونية.[388]

أهداف الدارسة

حيث أن الهدف من هذه الورقة تقديم دارسة مفصلة تسلط الضوء علي الاستراتيجية الموريتانية لأمن السيبراني في حماية التجارة الالكترونية في القانون الموريتاني و ذلك من خلال أهدافها ووسائل تحقيقها و هل سيمكن ذلك موريتانيا من حماية أمنها السيبراني ؟.

أهمية الدارسة

تكمن أهمية هذه الورقة في تزايد الاهتمام الوطني و الدولي لأمن السيبراني و محورية التجارة الالكترونية التي أصبحت مهمة جدا و خاصة بعد ظهور و باء كورونا الذي توقفت بسببه المبادلات التجارية التقليدية .

إشكالية الدارسة

أن الإشكالية المطروحة من خلال الورقة هي : هل استطاعت المنظومة القانونية الموريتانية مواكبة التحولات و التغيرات العالمية و التي أصبح محورها الأساسي الأمن السيبراني ؟.

1- استراتيجية الامن السيبراني : دارسة حالة المغرب إعداد : د. عبد الواحد البيديري - دكتوراه في القانون العام، جامعة سيدي محمد بن عبد الله، فاس، المغرب - باحث في العلاقات الدولية والعلوم السياسية- مجلة الدراسات الاستراتيجية والعسكرية : العدد الحادي عشر يونيو - حزيران , 2021المجلد 3 وهي مجلة ثلاثية دولية محكّمة تصدر من ألمانيا - برلين عن "المركز الديمقراطي العربي"

[387] - الأجندة الرقمية العربية و الاستراتيجية العربية لتكنولوجيا المعلومات و الاتصالات- المشروع المشترك للتعاون الفني بين الإسكوا وجامعة الدول العربية-2017

[388] - القانون رقم : 022/ 2018 الصادر بتاريخ 12 يونيو 2018 المتضمن المبادلات الإلكترونية

من خلال ما تقدم سنقوم بتقسيم هذه الورقة من خلال العناوين التالية :

- المبحث الأول : الإطار التنظيمي و المؤسسي و القانوني للاستراتيجية الموريتانية لأمن السيبراني

- المبحث الثاني : قانون المبادلات الالكترونية الموريتاني

- الخاتمة

المبحث الأول : الإطار التنظيمي و المؤسسي و القانوني للاستراتيجية الموريتانية لأمن السيبراني

سنتطرق من خلال المبحث هذا المبحث لإطار التنظيمي و المؤسسي و القانوني للاستراتيجية الموريتانية لأمن السيبراني و ذلك من خلال مطلبين هما :

المطلب الأول : الإطار التنظيمي و المؤسسي و المطلب الثاني : الإطار القانوني

المطلب الأول : الإطار التنظيمي و المؤسسي

حيث انه يعرف الأمن السيبراني بأنه عملية حماية الأنظمة والشبكات و البرامج ضد الهجمات الرقمية تهدف هذه الهجمات السيبرانية عادة إلى الوصول إلى المعلومات الحساسة أو تغيرها أو تدميرها بغرض الاستيلاء علي المال من المستخدمين أو مقاطعة عمليات الأعمال العادية .[389]

يمثل تنفيذ الأمن السيبراني تحديا كبيرا اليوم نظرا لوجود عدد أجهزة يفوق أعداد الأشخاص كما أصبح المهاجمون أكثر ابتكار.

و يعتبر الأمن السيبراني تحديا كبيرا بالنسبة للعالم وموريتانيا ليست بمنأى عن مواجهة تحدياته. و عيا منها بأهمية الأمن السيبراني في البلد و الحاجة إلى تأمين الفضاء الرقمي قررت الحكومة الموريتانية وضع استراتيجية أمنية إلكترونية .[390]

كما وضعت خطة عمل وطنية لتحقيق أهداف هذه الاستراتيجية و أنشئت وزارة للتحول الرقمي و الابتكار و عصرنة الإدارة. و قد قامت الدولة الموريتانية بوضع استراتيجية لأمن السيبراني وقد تم تحديدها ضمن خمسة مجالات عمل ستركز فيها جهود الدولة و مختلف الجهات المعنية على تجسيد هذه التوجيهات الاستراتيجية حتى العام 2022.

---

[389] موقع -https://www.cisco.com/c/ar_ae/products/security/what-is-cybersecurity.htm

[390] - الأجندة الرقمية العربية و الاستراتيجية العربية لتكنولوجيا المعلومات و الاتصالات- المشروع المشترك للتعاون الفني بين الإسكوا وجامعة الدول العربية-2017

و تغطي هذه الاستراتيجية هذه المحاور :

1- حماية أنظمة المعلومات الوطنية والحكومية

2- حماية البنى التحتية الحيوية

3- تطوير المهارات و الوعي

4- تطوير الإطار القانوني و التنظيمي

5- تطوير الشراكة بين القطاعين العام والخاص حول الأمن السيبراني و التعاون الدولي

المطلب الثاني : الإطار القانوني

لقد وضعت الدولة الموريتانية ترسانة قانونية متكاملة لأمن السيبراني تمثلت في المنظومات القانونية التالية:

1- القانون رقم : 006/ 2016 الصادر بتاريخ 20 يونيو 2016 المتضمن القانون التوجيهي لمجتمع المعلومات

2- القانون رقم : 007/ 2016 الصادر بتاريخ 20 يونيو 2016 المتضمن الجريمة السيبرانية

3- القانون رقم : 020 / 2017 الصادر بتاريخ 22 يوليو 2017 المتضمن حماية البيانات ذات الطابع الشخصي

4- القانون رقم : 022/ 2018 الصادر بتاريخ 12 يونيو 2018 المتضمن المبادلات الإلكترونية

5- القانون رقم : 025/ 2013 الصادر بتاريخ 15 يوليو 2013 المتضمن قانون الاتصالات الإلكترونية

6- القانون رقم : 015/ 2020 الصادر بتاريخ 23 يوليو 2020 المتضمن قانون مكافحة التلاعب بالمعلومات

7- - القانون رقم : 014 / 2021 الصادر بتاريخ 30 يوليو 2021 المتعلق بخدمات وسائل الدفع الإلكتروني

المبحث الثاني : قانون المبادلات الإلكترونية الموريتاني

لقد اصدرت الدولة الموريتانية القانون المتضمن المبادلات الالكترونية و هو يتعلق بحماية التجارة الإلكترونية.[391]

و قد عرف التجارة الإلكترونية بأنها نشاط اقتصادي بواسطته يقترح شخص طبيعي أو معنوي و / أو يؤمن عن بعد و بوسيلة إلكترونية توريد سلع و / أو توفير خدمات و يتكون القانون المذكور من مائة و ثلاثة مواد (103) و تسعة فصول (9) و هي :

1- أحكام عامة

---

[391] - القانون رقم : 022/ 2018 الصادر بتاريخ 12 يونيو 2018 المتضمن المبادلات الإلكترونية

2- المكتوب في شكل إلكتروني

3- مسؤولية موردي خدمات النفاذ و استضافة المواقع و البيانات

4- مسؤولية ناشري خدمات اتصال للجمهور علي الانترنت

5- التجارة الإلكترونية

6- الإشهار بطريقة إلكترونية

7- العقد بطريقة إلكترونية

8- تأمين المبادلات الإلكترونية

9- أحكام نهائية

و حيث أن المادة 2 منه نصت علي انه ينظم المبادلات الإلكترونية و الخدمات من خلال الوسائل الإلكترونية في الجمهورية الإسلامية الموريتانية و يطبق خصوصا علي :

أ- الخدمات بالطريقة الإلكترونية التي تؤدي إلى إبرام عقود لاقتناء سلعة أو تقديم خدمة أو توفر معلومات أو اشهارات أو أدوات تمكن من البحث عن البيانات أو النفاذ إليها أو استرجاعها أو تلك التي تتمثل في إرسال البيانات بواسطة شبكة اتصال إلكتروني أو توفير نفاذ إلى أي شبكة أو ضمان تخزين البيانات و لو كانت تلك الخدمات غير معوضة من قبل الذين يستلمونها.

ب- إزالة الطابع المادي للإجراءات الإدارية .

و حيث أن المجالات التي لا تدخل في ميدان تطبيقه نصت عليها المادة 3 منه و هي :

أ- أنشطة التمثيل و المساعدة أمام العدالة

ب- الأنشطة التي يمارسها الموثقون طبقا للنصوص المعمول بها

و حيث أننا سنتطرق للقانون المذكور من خلال مطلبين هما :

المطلب الأول : أحكام عامة و الشكل الالكتروني و مسؤولية موردي الخدمات و ناشري الخدمات

أ- **أحكام عامة و المكتوب في الشكل الإلكتروني**

حيث أن فصل الأحكام العامة لقانون المبادلات الالكترونية هو الفصل الأول ومنظم بالمواد من 1 إلى 3 و يتكون من قسمين هما :

-1- التعريفات **-2-** هدف و مجال تطبيقه .

أما الفصل المتعلق بالمكتوب في شكل إلكتروني فمنظم من المواد 4 إلي 24 ويتكون من قسمين هما :

- **1**- الشكل بالطريقة الإلكترونية - **2**- الإدارة الإلكترونية .

و قد نصت المادة 4 منه علي انه :

ما لم تنص أحكام تشريعية علي خلاف ذلك لا يمكن إجبار أي شخص علي تقديم عقد قانوني عن طريق إلكتروني . تكون الموافقة علي إرسال أو استقبال اتصالات بالطريق الالكتروني صريحة في غياب ذلك ، يمكن استنتاج موافقة الشخص من خلال سلوكه الظرفي.

كما نصت المادة 5 علي أنه :

إذا كانت هناك أحكام قانونية أو تنظيمية تنص علي وجوب شكل خاص لوضع عقد قانوني خاص لإغراض الصلاحية أو الإثبات أو الإشهار أو الحماية أو الإعلام ، فإن ذلك الشرط يمكن استيفاؤه بالطريق الإلكتروني حسب الفرضيات و الشروط المنصوص عليها في – النظائر الوظيفية – الموجودة في الأحكام التالية من هذا القسم. وحيث أن المادة 6 نصت علي الاستثناء من خلال ما يلي :

تستثنى من أحكام المادة السابقة من هذا القانون :

أ- العقود العرفية المتعلق بقانون الأسرة و الميراث

ب- العقود العرفية المتعلقة بالضمانات الشخصية أو العينية ذات الطابع المدني أو التجاري ، إلا إذا كانت مبرمة من قبل شخص لأغراض مهنته .

ج- العقود التي تنشئ أو تحول حقوقا عينية على ممتلكات ثابتة .

د- العقود القانونية التي يطلب القانون بموجبها تدخل المحاكم .

ه- الإجراءات القضائية.

إذا كانت هناك أحكام قانونية أو تنظيمية تنص علي وجوب شكل خاص لوضع عقد قانوني خاص لإغراض الصلاحية أو الإثبات أو الإشهار أو الحماية أو الإعلام ، فإن ذلك الشرط يمكن استيفاؤه بالطريق الإلكتروني حسب الفرضيات و الشروط المنصوص عليها في – النظائر الوظيفية – الموجودة في الأحكام التالية من هذا القسم. أما المادة 7 من قانون المبادلات الإلكترونية فقد نصت علي انه :

ينتج المكتوب علي سلسلة من الحروف أو علامات أو الأرقام أو أية إشارات أو رموز ذات معنى مفهوم ، مهما كانت دعامتها أو طرق إرسالها.

أما الإدارة الإلكترونية فقد نصت المادة 16 علي انه : يقبل المكتوب الإلكتروني في جميع مبادلات المعلومات أو الوثائق أو العقود الإدارية و يمكن القيام بإرساله بطريقة إلكترونية . ولهذا الغرض تقوم كل إدارة بتبليغ العناوين الإلكترونية التي تمكن من الاتصال بها . و علاوة على ذلك ، فإن أي شخص طبيعي أو معنوي يرغب في الاتصال به من قبل الإدارة بواسطة البريد الإلكتروني ، يبلغنا العناوين الضرورية لذلك و يسهر علي المراجعة المنتظمة لبريده الإلكتروني ، و يشعر الإدارة بكل تغيير في العناوين.

ب- مسؤولية موردي خدمات النفاذ و استضافة المواقع و البيانات و مسؤولية ناشري خدمات اتصال للجمهور علي الإنترنت

لقد نظم قانون المبادلات الإلكترونية مسؤولية موردي خدمات النفاذ و استضافة المواقع و البيانات ومسؤولية ناشري خدمات اتصال للجمهور علي الإنترنت من المواد 25 إلى 39 . يتكون الفصل المتعلق بمسؤولية موردي خدمات النفاذ و استضافة المواقع و البيانات من ثلاثة أقسام و هي:

-1- مسؤولية و التزامات موردي خدمات النفاذ المشعلون في مجال الاتصالات الإلكترونية .

-2- مسؤولية و التزامات المضفين -3- المسؤولية و الالتزامات المطبقة علي جميع موردي الخدمات .

أما الفصل المتعلق بمسؤولية ناشري خدمات اتصال للجمهور علي الإنترنت فقد نظمته المواد من 37 إلى 39 من قانون المبادلات الإلكترونية.

المطلب الثاني : التجارة الإلكترونية والإشهار و العقد بطرق إلكترونية و تأمين المبادلات الإلكترونية

الفصول المتعلقة بالتجارة الإلكترونية والإشهار و العقد بطرق إلكترونية و تأمين المبادلات الإلكترونية منظمة من المادة 40 إلى 101 بقانون المبادلات الإلكترونية سنقوم بالتطرق له من خلال ما يلي :

أ- التجارة الإلكترونية والإشهار بطريقة إلكترونية

حيث أن الفصل المتعلق بالتجارة الإلكترونية من ثلاثة أقسام و هي :

-**1**- مجال التطبيق – **2**- مدى حرية التجارة الإلكترونية -**3**– مبدأ الشفافية .

و لقد نصت المادة 40 من قانون المبادلات الإلكترونية علي أن :

تطبق أحكام هذا القسم علي التجارة الإلكترونية كما هى محددة في النقطة 3 من المادة الأولى من هذا القانون و التي تمارس فوق الجمهورية الإسلامية الموريتانية.

كما نصت المادة 41 علي انه :

يمارس نشاط التجارة الإلكترونية بحرية فوق التراب الوطني باستثناء المجالات المذكورة في المادة 3 من هذا القانون . تخضع الأنشطة التي تدخل ضمن التجارة الإلكترونية لقانون الدولة التي يقيم فيها الشخص الذي يمارسها ، مع مراعاة الرغبة المشتركة لهذا الشخص و كذا الشخص الملتقى للسلع و الخدمات.

أما في ما يخص تعريف الإشهار بطريقة إلكترونية فقد نصت عليه المادة 46 علي أنه :

كل إشهار ، مهما كان شكله ، يمكن النفاذ إليه بواسطة خدمة اتصال للجمهور علي الإنترنت ، يجب أن يمكن من التعرف عليه بشكل واضح بأنه كذلك و يجب أن يمكن بوضوح من معرفة الشخص الطبيعي أو المعنوي الذي تم إنجازه لحسابه . يجب أن تمكن أشكال الإشهار ، وخاصة العروض الترويجية الموجهة بواسطة البريد الإلكتروني أو بأية طريقة تقنية أخرى ، من التعرف عليها بشكل واضح و بدون التباس حول موضوع الرسالة فور استلامها من قبل المرسل إليه ، أو في حالة الاستحالة التقنية ، في مضمون الرسالة . تفسر أحكام هذه المادة دون المساس بالقوانين و النظم المعمول بها التي تعاقب الممارسات التجارية الخادعة.

ب- العقد بطريقة إلكترونية وتأمين المبادلات الإلكترونية

لقد نظم قانون المبادلات الإلكترونية من المواد 52 إلى 75 العقد بطريقة إلكترونية وتأمين المبادلات الإلكترونية. و يتكون الفصل المتعلق بالعقد بطريقة إلكترونية من خمسة أقسام وهي :

-**1**- المبدأ – تبادل المعلومات في العقود بالطريقة الإلكترونية -**2**– إبرام العقود بالطريقة الإلكترونية –**3**- حق التراجع -**4**– تنفيذ العقود المبرمة بالطريقة الإلكترونية.

حيث نصت المادة 52 علي انه :

يقبل العقد المبرم بطريقة إلكترونية مثل العقد المخطوط علي ورق إلا أن العقد الإلكتروني لا يمكن أن يخص مبادلات تتعلق ب:

1- إنشاء أو تحويل الممتلكات الثابتة باستثناء الإيجار

2- أي مجال أخر ينص القانون علي صيغة تعاقدية خاصة له

3- الأنشطة المستبعدة في المادة 3 من هذا القانون.

كما نصت المادة 53 من قانون المبادلات الإلكترونية المتعلقة بتبادل المعلومات في العقود بالطريقة الإلكترونية علي ما يلي :

إن المعلومات المطلوبة من أجل إبرام عقد أو تلك الموجهة خلال تنفيذه يمكن إرسالها بواسطة البريد الإلكتروني إذا كان مستقبلها قد قبل استخدام تلك الوسيلة . إن المعلومات الموجهة لمهني يمكن إرسالها إليه بواسطة البريد الإلكتروني مادام قد أبلغ عنوانه الإلكتروني المهني .

إذا كان يجب وضع هذه المعلومات في شكلية ، فإن هذه الشكلية توضع ـ بطريقة إلكترونية ، تحت تصرف الشخص الذي تجب عليه تعبئتها. و قد نصت المادة 56 علي إبرام العقود بالطريقة الإلكترونية حيث نصت علي انه :

لا يحتج بالشروط التعاقدية لمورد السلع أو الخدمات علي شريكه في التعاقد إلا إذا كان هذا الأخير قد توفر علي إمكانية الاطلاع عليها قبل إبرام العقد و كان قبوله صريحا و تبلغ له كتابيا بطريقة تمكنه من حفظها و استنساخها.

كما بينت المادة 57 إبرام العقد علي انه :

لكي يكون العقد مبرما بشكل صحيح ، يجب أن يتوفر مستقبل العرض علي إمكانية التأكد من تفاصيله طلبيته و سعرها الإجمالي و كذلك إمكانية فرض تصحيح الأخطاء المحتملة ، قبل تأكيد الطلبية للتعبير عن عن قبوله .يجب على صاحب العرض تقديم إفادة بالاستلام دون تأخير غير مبرر و بالطريقة الإلكترونية ، للطلبية التي أرسلت إليه بهذه الطريقة . و تشمل إفادة الاستلام هذه المعلومات :

أ- الهوية و العنوان الجغرافي لمورد السلع أو الخدمات .

ب- المواصفات الأساسية للسلعة أو الخدمة المطلوبة .

ج- سعر السلعة أو الخدمة بما فيه جميع الرسوم .

د- و عند الاقتضاء مصاريف التسليم

ه- طرق التسديد أو التسليم أو التنفيذ .

و- عند الاقتضاء شروط و طرق ممارسة حق التراجع .

ز- المعلومات التي تمكن مستقبل السلعة أو الخدمة من تقديم مطالباته وخاصة رقم هاتف و عنوان إلكتروني و عنوان جغرافي.

ح – المعلومات المتعلقة بالضمانات بخدمة ما بعد البيع التجارية الموجودة .

ط – شروط فسخ العقد إذا كانت مدته غير محدودة أو تتجاوز سنة .

تعتبر الطلبية و تأكيد قبول العرض و إفادة الاستلام قد استلمت عندما تستطيع الأطراف المرسلة إليهم النفاذ إليها . تقدم المعلومات الموجودة في إفادة الاستلام بطريقة تمكن من حفظها و استنساخها.

نصت المادة 58 من قانون المبادلات الإلكترونية علي انه يتم الخروج على أحكام المادة السابقة عندما يتم إبرام العقد حصريا بالطريقة الإلكترونية من خلال استخدام الهاتف الجوال و في هذه الحالة لا تشمل إفادة الاستلام إلا البيانات التالية :

أ- هوية المرسل إليه

ب- وصف السلعة أو الخدمة المطلوبة

ج- السعر الإجمالي للسلعة أو الخدمة ، بما فيه جميع الرسوم و الأعباء و تكاليف التسليم و العمولات و النفقات المتعلقة به .

د- وجود أو غياب حق التراجع .

ه- العناوين التي تمكن مستلم الخدمة أو السلعة من الحصول على مزيد من المعلومات و خاصة تلك المبينة في المادة السابقة .

ونصت ايضا المادة 59 علي انه يجب علي البائع ، قبل إبرام العقد تمكين المستهلك من التلخيص النهائي لمجموع خياراته و تأكيد الطلبية أو تعديلها حسب إرادته و مراجعة الإفادة الإلكترونية المتعلقة بتوقيعه .

أما حق التراجع فقد نصت عليه المادة 63 حيث نصت علي انه و من دون المساس بأحكام قانون الالتزامات و العقود وكافة الأحكام الأخرى المعمول بها ، يستطيع أن يتراجع خلال أجل مدته عشرة (10) أيام عمل تبدأ:

- اعتبارا من تاريخ استلامها بالنسبة للمنتجات .
- اعتبارا من تاريخ إبرام العقد بالنسبة للخدمات .

يتم إبلاغ التراجع بواسطة أي وسيلة منصوص عليها مسبقا في العقد و في هذه الحالة ، يلزم البائع بتعويض المبلغ الذي دفعه المستهلك خلال عشرة (10) أيام عمل اعتبارا من تاريخ إرجاع المنتج أو التراجع عن الخدمة و يتحمل المستهلك مصاريف إعادة المنتج .

و في ما يتعلق بتنفيذ العقود المبرمة بالطريقة الإلكترونية نصت المادة 69 من قانون المبادلات الإلكترونية يحظر علي البائع تسليم منتج غير مطلوب من قبل المستهلك إذا كان مرفقا بطلب التسديد .في حالة تسليم منتج غير مطلوب من قبل المستهلك ، لا يمكن أن يطالب هذا الأخير بدفع سعره أو تكلفة تسليمه .

كما نصت المادة 70 بغض النظر عن تعويض الضرر لفائدة المستهلك ، يستطيع هذا الأخير إعادة المنتج بحالته إذا كان غير مطابق للطلبية أو إذا كان البائع لم يحترم آجال التسليم .

أما الفصل الثامن المعنون بتأمين المبادلات الإلكترونية فيتكون من أربعة أقسام هي :

-**1**- الدليل الإلكتروني -**2**- التوقيع الإلكتروني -**3**- الإفادة الإلكترونية -**4**- مقدمي خدمات التصديق الإلكتروني .

نصت المادة 76 منه علي انه يثبت الدليل الكتابي أو الدليل الحرفي طبقا لأحكام المادة 7 من هذا القانون.

كما نصت المادة 77 علي انه يقبل المكتوب بالطريقة الإلكترونية دليلا بنفس درجة المكتوب على دعامة ورقية و يمتلك نفس القوة المثبتة ، شريطة تمكينه من التعرف القانوني على الشخص الصادر عنه ، و أن يكون تم إعداده و حفظه ضمن الشروط الكفيلة بضمان سلامته .

و نصت المادة 82 علي انه لا يمكن إجبار أحد علي التوقيع الكترونيا و مع ذلك يمكن أن يكون عقود السلطات الإدارية موضوع توقيع إلكتروني حسب الشروط المنصوص عليها في الترتيبات التنظيمية .

و نصت المادة 83 بانه يعرف التوقيع الضروري لاكتمال عقد قانوني صاحب التوقيع . و يبرز موافقة الأطراف على الالتزامات الناتجة عنه . و عندما يتم و ضعه من قبل مأمور عمومي فإنه يضفي علي العقد الطابع الرسمي.

إذا كان التوقيع إلكترونيا، فإنه يتمثل في استخدام طريقة ذات مصداقية للتعريف تضمن علاقته بالعقد الذي يرتبط به . تفترض مصداقية هذه الطريقة ، حتي يثبت العكس ، عندما يتم إنشاء التوقيع الإلكتروني .

يمكن إعداد العقد الرسمي علي دعامة إلكترونية إذا كان معدا و محفوظا حسب الشروط المحددة بالطرق التنظيمية .

كما نصت المادة 84 علي انه دون المساس بالأحكام المعمول بها ، فإن التوقيع الإلكتروني المؤمن المنشأ بواسطة نظام لإنشاء التوقيع الآمن و الذي يستطيع الموقع حفظه تحت رقابته الحصرية و الذي يعتمد تدقيقه علي إفادة مؤهلة يقبل كتوقيع مثل التوقيع اليدوي .

نصت المادة 88 علي الإفادة الإلكترونية علي انه لا يمكن اعتبار الإفادة الإلكترونية مؤهلة إلا كانت صادرة عن مقدم خدمات تصديق مؤهل و إذا كانت تشمل البيانات الواردة في المادة التالية من هذا القانون.يعتبر مؤهلا مقدم التصديق خدمة التصديق الذي :

أ- يمتثل لأحكام المادة 92 من هذا القانون

ب- يكون موضوع اعتماد ، حسب الشروط التنظيمية .

المادة 89 نصت علي انه تشمل الإفادة الإلكترونية المؤهلة البيانات التالية :

أ- بيانا يشير إلى أن هذه الإفادة تم تسليمها بصفتها إفادة إلكترونيها مؤهلة .

ب- هوية مقدم خدمات التصديق الإلكتروني و كذا الدولة التي يقيم فيها .

ج- اسم الموقع و عند الاقتضاء صفته .

د- بيانات تدقيق التوقيع الإلكتروني المطابقة لبيانات إنشائه .

ه- تحديد بداية و نهاية فترة صلاحية الإفادة الإلكترونية و كذا رمز تعريفها .

و- التوقيع الإلكتروني المؤمن لمقدم خدمات التصديق الذي سلم الإفادة الإلكترونية .

ز- شروط استخدام الإفادة الإلكترونية ، و خاصة المبلغ الأقصى للمبادلات التي يمكن استخدام هذه الإفادة لها .

نصت المادة 92 من قانون المبادلات الإلكترونية علي أنه :

يستوفي مقدم خدمات التصديق الإلكتروني الشروط التالية :

أ- إثبات مصداقية خدمات التصديق الإلكتروني التي يوردها .

ب- ضمان تسيير سجل الإفادات الإلكترونية سريع و مؤمن لفائدة الأشخاص الذين يطلبون ذلك و الذين تسلم لهم إفادة إلكترونية .

ج- ضمان سير عمل خدمة يمكن النفاذ إليها في أي وقت و تمكن الشخص الذي سلمت له الإفادة الإلكترونية من أن يلغي هذه الإفادة بدون تأخير و بشكل مؤكد .

د- السهر علي أن يكون تاريخ و ساعة تسليم و إلغاء الإفادة الإلكترونية مبين بشكل واضح

ه- تطبيق إجراءات السلامة المناسبة و استخدام النظم و المنتجات التي تضمن الأمن التقني و التشفيري للوظائف التي يقدمونها .

و- اتخاذ أي إجراء كفيل بتفادي تزوير الإفادات الإلكترونية.

ز- ضمان سرية بيانات إنشاء التوقيع الإلكتروني خلال عملية إنشاء تلك البيانات والامتناع عن حفظ أو استنساخ تلك البيانات في الحالة التي يقدمها للموقع .

ح – السهر في حالة القيام معا بتوفير بيانات إنشاء و بيانات تدقيق التوقيع الإلكتروني علي أن تكون بيانات الإنشاء مطابقة لبيانات التدقيق.

ط- الحفظ بطريقة إلكترونية ، لكامل المعلومات المتعلقة بالإفادة الإلكترونية والتي قد تكون ضرورية لإثبات التصديق الإلكتروني أمام القضاء .

ي- استخدام نظم لحفظ الإفادات الإلكترونية تضمن أن :

1- يخصص إدخال و تعديل البيانات فقط للأشخاص المرخص لهم لذلك الغرض من قبل مقدم الخدمة .

2- لا يمكن أن يتم نفاذ الجمهور إلى إفادة إلكترونية بدون الموافقة المسبقة لصاحب الإفادة

3- يمكن اكتشاف أي تعديل من شأنه الإخلال بأمن النظام.

ك- تدقيق هوية الشخص الذي سلمت له إفادة إلكترونية من خلال مطالبته بتقديم وثيقة هوية رسمية ، من جهة و الصفة التي يدعيها هذا الشخص من جهة أخرى ، و حفظ مواصفات و مراجع الوثائق المقدمة لإثبات تلك الهوية و تلك الصفة .

ل- التأكد عند تسليم الإفادة الإلكترونية بأن المعلومات التي تحتوي عليها صحيحة و أن الموقع المعرف فيها يمتلك بيانات إنشاء التوقيع الإلكتروني المطابقة لبيانات تدقيق التوقيع الإلكتروني الموجود في الإفادة

م- التقديم كتابيا للشخص الذي يطلب إصدار إفادة ، قبل إبرام عقد خدمات التصديق الإلكتروني بلغة سهلة الفهم ، المعلومات المتعلقة بإجراءات و شروط استخدام الإفادة و تلك المتعلقة بإجراءات الاعتراض و تسوية النزاعات .

ن- توفير المعلومات المنصوص عليها في النقطة السابقة للأشخاص الذين يعتمدون على إفادة إلكترونية .

حيث انه و باختصار شديد تم التطرق لقانون المبادلات الإلكترونية الموريتاني.

الخاتمة

يتضح مما تقدم أن الأمن السيبراني أصبح ضرورة عالمية حتمية وأن إستراتيجية الأمن المعتمدة بموريتانيا مازالت في البداية أي بعبارة أدق دون المستوى المطلوب .

وقد اتضح ذلك من خلال ترتيب موريتانيا في المؤشر العالمي للأمن السيبراني الصادر عن الاتحاد الدولي للاتصالات من خلال التقرير الأخير .

حيث وصلت إلى رقم 133 من التريب العالمي مما يحتم عليها مزيدا من العمل و التنسيق مع الدول الصديقة من أجل الاستفادة من تجاربها.

و أما في ما يخص قانون المبادلات الالكترونية فانه بحاجة إلي التطبيق و الممارسة ومواكبة التطورات العالمية و كذلك إصدار مراسيم تطبيقية له .

انطلاقا مما تقدم أتقدم إليكم بالمقترحات و التوصيات التالية :

1- نشر الوعي بخطورة الجريمة السيرانية

2- عدم الخلط بين حرية التعبير و الجريمة السيبرانية

3- تفعيل منتدى الأمن الرقمي العربي

4- إنشاء وزارة مختصة بالأمن السيبراني

5- إدماج تخصص الأمن السيبراني بالجامعة

6- إنشاء معهد متخصص بالأمن السيبراني

7- إنشاء مفوضية شرطة خاصة في مكافحة الجريمة السيبرانية

8- إنشاء نيابة عامة و قضاء تحقيق و محكمة مختصة للنظر في قضايا الجريمة السيبرانية

9- تفعيل قانون المبادلات الإلكترونية و إصدار مراسيم تطبيقية له

10- إنشاء محكمة عربية مختصة للنظر في قضايا الجريمة السيبرانية

11- إنشاء شرطة عربية مختصة في محاربة الجريمة السيبرانية

12- القيام بندوات و مؤتمرات حول الأمن السيبراني

و في نهاية مداخلتي هذه المتواضعة أشكر القائمين علي هذا المؤتمر العلمي الهام والمفيد و بالخصوص الدكتور ضياء نعمان و أملي كبير في أن أكون قد تقدمت بما يفيد.

قائمة المراجع و المصادر

أ- القوانين

1- القانون رقم : 006/ 2016 الصادر بتاريخ 20 يونيو 2016 المتضمن القانون التوجيهي لمجتمع المعلومات

2- القانون رقم : 007/ 2016 الصادر بتاريخ 20 يونيو 2016 المتضمن الجريمة السيبرانية

3- القانون رقم : 020 / 2017 الصادر بتاريخ 22 يوليو 2017 المتضمن حماية البيانات ذات الطابع الشخصي

4- القانون رقم : 022/ 2018 الصادر بتاريخ 12 يونيو 2018 المتضمن المبادلات الإلكترونية

5- القانون رقم : 025/ 2013 الصادر بتاريخ 15 يوليو 2013 المتضمن قانون الاتصالات الإلكترونية

6- القانون رقم : 015/ 2020 الصادر بتاريخ 23 يوليو 2020 المتضمن قانون مكافحة التلاعب بالمعلومات

7- القانون رقم : 014 / 2021 الصادر بتاريخ 30 يوليو 2021 المتعلق بخدمات وسائل الدفع الإلكتروني

ب- الكتب و التقارير و الدوريات و المواقع الإلكترونية

1- الأجندة الرقمية العربية و الاستراتيجية العربية لتكنولوجيا المعلومات و الاتصالات- المشروع المشترك للتعاون الفني بين الإسكوا وجامعة الدول العربية-2017

2- تقرير مؤشر الأمن السيبراني الصادر عن الاتحاد الدولي للاتصالات

3- استراتيجية الامن السيبراني : دارسة حالة المغرب إعداد : د. عبد الواحد البيديري – دكتوراه في القانون العام، جامعة سيدي محمد بن عبد الله، فاس، المغرب – باحث في العلاقات الدولية والعلوم السياسية- مجلة الدراسات الاستراتيجية والعسكرية : العدد الحادي عشر يونيو – حزيران 2021 , المجلد 3 وهي مجلة ثلاثية دولية محكّمة تصدر من ألمانيا – برلين عن "المركز الديمقراطي العربي.

4- موقع - https://www.cisco.com/c/ar_ae/products/security/what-is-cybersecurity.htm

حماية المستهلك الإلكتروني من الإعلانات المضللة عبر الإنترنت

إيهاب أحمد محمد عبد الوهاب
باحث قانوني بديوان عام المحافظة كفر الشيخ- مصر

المقدمة

الحمد لله الذي جل عن الأنداد وتنزه عن أن يكون له نظير من العباد، وأشهد أن لا إله إلا الله وحده لا شريك له. شهادة من عرف المعنى منها والمراد، واعتَقد ما دلت عليه حقيقة الاعتقاد، وأشهد أن محمدا عبده ورسوله، الهادي إلى سبل الرشاد، صلى الله عليه وعلى آله وأصحابه وسلم تسليماً كثيراً.

فى ضوء النظرية التقليدية للالتزامات والقواعد العامة فى الإحكام العقابية فى حماية المستهلك الالكتروني، والتطور التقني الحديث أدى كلاهما الى صدور العديد من التشريعات الخاصـــة بحماية المستهلك، فالمتغيرات الجنائية التي نتجت عن استخدام التكنولوجيا الحديثة فى الإلكتـــرونية، وخصوصا في السنوات القليلة الماضية أسهمت فى ظهور العديد من المشكلات العملية التي تواجه المستهلك عند التعاقد الالكتروني.

من المعلوم ان المستهلك يبدأ عملية الشراء باختيار السلعة أو الخدمة التي يمكن لها أن تشبع حاجته، وبالتالي فإنه يبحث عن تلك السلع أو الخدمات التي يكون في حاجة لها، ومع انتشار الإنترنت واستخدامه في التجارة الإلكترونية من خلال عرض السلع عبر شبكة الإنترنت، ظهرت العديد من الصفحات والتبويبات الإعلانية الكاذبة والمضللة التي تجذب المستهلك إليها، ولكنها في النهاية تكون إما مزيفة أو وهمية أو لأي غرض غير مشروع أخر.

فقد أيقن الصناع والمنتجون في شتى المجالات ما للإعلان من أهمية في العصور الحديثة مما له من وظيفة تسويقية فالإعلان من أهم وسائل إثارة الطلب على السلع والخدمات، فالإعلان جزءا أساسيا من حياتنا اليومية نظرا لأن العملية التجارية الإلكترونية تتكون من مستهلك إلكتروني منتج وتاجر وصانع ووسيط، فهو وسيلة إعلام وجمع المستهلكين بما تشتمل عليه المنتجات والخدمات التي يرغب التجار والمنتجون في تقديمها

لهم، ويتنوع الإعلان بشتى الصور فمنها مثلا الإعلان عبر الانترنت والراديو والتلفزيون والمجلات والجرائد والأجهزة اللوحية وجميع وسائل الاتصال الحديثة.[392]

أهمية الموضوع:

وتتجلى اهمية موضوع الحماية الجنائية للمستهلك من الاعلانات المضللة في الآتي:

- إن موضوع الحماية الجنائية للمستهلك في مجال الاعلانات يستمد أهميته بالأساس من المكانة التى يحتلها الفرد في الدولة، والذي يتعرض للكثير من هذه الجرائم في حياته اليومية، والتى تتعلق بأسمي حقوقة، وبلك تزداد الحاجة الى حاجة المستهلك الى تشريع جنائي يحمية من هذا التهديد.

- تبرز أهمية الموضوع ايضا فى انه موضوع المجتمع بأسره باعتبارنا جميعا مستهلكون، فالاعلانات التجارية في عصرنا أصبحت المتحدث الرسمي عن نشاط الشركات والأفراد.

- أصبحت الإعلانات التجارية أيضا وسيلة المستهلكين للتعرف على السلع الخدمات المعروضة الكترونيا، فهو اداة استشارية عند اتخاذ القرارات الاستهلاكية، لذا يجب ان يجدها من مصدر موثوق وصادق وليس مصدر كاذب ومضلل، هدفه سلب أموال المستهلك الإلكتروني.

أسباب اختيار الموضوع:

تتمثل أسباب إختيار الموضوع في أسباب موضوعية وأخرى ذاتية، ومن أهم الأسباب الموضوعية ما يلي:

- التوجه الاقتصادي الحالي لمصر وما تشهده من حرية حركة السلع والخدمات والتنوع الموجود في السوق من منتجات مستوردة ومحلية، مما قد يؤدي بفئة من التجار وسعيا للربح السريع إلى إستخدام وسائل غير مشروعة والتي تتمثل في إصدارهم إعلانات كاذبة ومضللة للسيطرة على نفسية المستهلك الإلكتروني.
- ارتفاع نسبة قضايا جريمة الإعلانات الكاذبة والخادعة في العالم وهذا يرجع لما نشهده يوميا من إكتشاف للسلع المغشوشة على مستوى الإنتاج أو على مستوى التسويق.
- قصور الحماية المدنية للمستهلك وعدم كفايتها لأن هذه الحماية تفترض وجود عقد بين المنتج أو الناقل أو الموزع والمستهلك وهي قاصرة على طرفي العقد فقط دون باقي جمهور المستهلكين.

---

[392] د/ محمد أحمد محمود ابو الهنا، حماية المستهلك في مرحلة ما قبل إبرام العقد، رسالة دكتوراه، جامعة عين شمس، 2019، ص65.

أما بالنسبة للأسباب الذاتية فتتمثل فيما يلي: الرغبة والإهتمام بموضوع حماية المستهلك فهو موضوع حيوي يمس جميع مستهلكي العالم، وايضا الانتشار الكبير للخداع والكذب في الحياة الاستهلاكية ومن خلالها كثرة الجرائم الماسة بالمستهلك.

أهداف الدراسة:

تهدف هذه الدراسة إلى:

- تبيان القانون الذي يحمي المستهلك من الإعلانات التجارية الكاذبة والمضللة، وما تلحقه من أضرار وأيضا تنوير المستهلك بالإجراءات المتبعة عندما يقع في إشهار كاذب ومضلل.
- توعية المستهلكين بأن هناك قانون يحميهم من خطر الإعلانات الكاذبة والمضللة.
- تحديد الجزاءات الجنائية لكل مرتكب لجريمة الإعلان الكاذب والمضلل.
- تحديد الحالات التي يعتبر فيها الإعلان كاذب ومضلل.

إشكالية البحث:

يتعين علينا في إطار هذا البحث والذي يتمحور موضوعه في الحماية الجزائية للمستهلك من الإعلان الكاذب والمضلل طرح الإشكالية التالية:

- ما مدى فاعلية النصوص الواردة فى القوانين في حماية المستهلك من الإعلانات التجارية الكاذبة والمضللة؟
- وللإجابة على عن هذه الاشكالية نطرح بعض التساؤلات الفرعية والمتمثلة في:
- ما مفهوم جريمة الإعلان الكاذب والمضلل، وما هي أركانها؟
- وما هي المسؤولية الجنائية المطبقة على الأشخاص الذين يرتكبونها وفيما تتمثل العقوبة المقررة لها؟
- وماهي الهيئات التي عينها المشرع لحماية المستهلك منها؟

منهج البحث:

في سبيل البحث عن الاجابة لهذه الإشكالية اتبعنا المنهج التحليلي والمقارن وذلك من خلال تحليل ومقارنة بعض النصوص القانونية التي تعالج هذا الموضوع.

خطة البحث:

وعلي إثر ذلك نقسم دراستنا في هذا البحث إلي: (المبحث الأول) ماهية الإعلانات المضللة، بينما (المبحث الثاني) وسائل حماية المستهلك الإلكتروني من الإعلانات المضللة.

المبحث الأول: ماهية الإعلانات المضللة

تُسبق العملية التجارية التي تتم عبر الإنترنت -غالبا- بصورة من صور الدعاية والإعلان عبر شبكة الإنترنت، ومما لا شك فيه أن الدعاية والإعلان أصبحت من أهم آليات النظام التجاري التي لا يمكن الاستغناء عنها في المنافسة وتحقيق الربح والعرض عبر الشبكات الإلكترونية[393]، لذلك سأتناول في هذا المبحث مفهوم الإعلان الإلكتروني (المطلب الأول). وطبيعته القانونية (المطلب الثاني)، حماية المستهلك الإلكتروني جنائيا من الإعلان المضلل (المطلب الثالث).

المطلب الأول: مفهوم الإعلان الإلكتروني

بصفة عامة يكون الإعلان موجه للمستهلك، بينما الإعلان الموجه للمستهلك الإلكتروني يكون نتاج عقد محل أبرامه الإنترنت أو أي وسيلة إلكترونية أخرى استخدمت في إتمام العقد، فالعقد المبرم هنا ينشأ مثله مثل سائر العقود بإيجاب يطابق قبول بين طرفي العقد المُعلن ووكالة الإعلان، وهو من العقود الرضائية التي ليس لها شكل محدد، ولا يشترط شكل إجرائي معين لإبرامها، كما لم تضع التشريعات المقارنة تنظيما خاصا لها، لذلك فإن أغلب الفقه يرى أنها من العقود غير المسماة [394].

لهذا فإن مثل تلك العقود قد تثير مجموعة من الصور الإجرامية التي سوف نقوم بتوضيحها بعد ذلك، إلا أننا في هدى ما سبق سوف نقسم هذا المطلب إلي فرعين، ندرس في الأول تعريف الإعلان الإلكتروني المضلل، ثم نخصص الثاني لبحث وسائل الإعلان الإلكتروني.

الفرع الأول: تعريف الإعلان الإلكتروني المضلل

لم يضع المشرع تعريفاً محدداً للإعلان، إلا أن بعض الفقه قد عرف الإعلان بأنه " كل وسيلة تهدف إلى التأثير نفسيا على الجمهور لتحقيق غايات تجاري[395]، ويعرف كذلك بأنه "عبارة عن مجموعة من الجهود غير

---

(393) د/ خالد ممدوح إبراهيم، حماية المستهلك في المعاملات الإلكترونية، الدار الجامعية، الإسكندرية، 2007، ص 79.

(394) د/ خالد ممدوح إبراهيم، حماية المستهلك في المعاملات الإلكترونية، المرجع السابق، ص83.

(395) د/ خالد ممدوح إبراهيم، حماية المستهلك في المعاملات الإلكترونية، مرجع سابق، ص 81.

الشخصية التي تهدف إلي توجيه انتباه أفراد المجتمع إلي سلعة ما، أو خدمة محددة لحثهم علي شرائها، أو طلبها، كما يعرف أيضا بأنه عبارة عن أنواع الأنشطة المختلفة التي يتم من خلالها نشر، أو إذاعة الرسائل الإعلانية المرئية أو المسموعة علي أفراد المجتمع بهدف حثهم علي شراء السلعة، أو الخدمة المعلن عنها"[396].

كما يعرف أيضا بأنه" فن تعريف الجمهور بمنتج لبيعه بشكل أوسع". أيضا عرفه الفقه الفرنسي بأنه "مجموعة الوسائل الوسائل الفنية ذات الأثر الجماعي المستخدمة لمصلحة منشأة أو مجموعة منشآت بغرض اكتساب أو زيادة أو الابقاء على عميل" [397].

يتضح من التعريفات السابقة على الرغم من قصورها في وضع تعريف جامع مانع يشمل كل جوانب الإعلان الإلكتروني بينما أهتم المشرع والفقه الفرنسي بتعريف الاعلان تعريفا جامعا ومانعا يشمل كل عناصر الخداع أو التضليل الإعلاني على عكس المشرع المصري قبل عام 2018، فمن المعروف أن الإعلان هو الوسيلة التي تستخدم لجذب أكبر عدد من المستهلكين، كما أن الهدف من الإعلان هو إقناع المستهلك بما تحققه تلك السلعة أو الخدمة له من مزايا أو ما يمكن أن تحققه له من فوائد، أيا كانت الوسيلة المستخدمة في ذلك، فما جاء به القانون رقم 181 لسنة 2018 ، لم يزد الا الإعلان بالوسائل الرقمية حيث جعل الإعلان بكافة الطرق بكافة الأساليب منها الإعلان عن طريق الوسائل الرقمية حيث جاء عام عكس القانون 66 لسنة 1956.

ولهذا فإننا نرى أن الإعلان الإلكتروني لا يختلف عن الإعلان في صورته التقليدية إلا في وسيلة نشر هذا الإعلان، فالإعلان التقليدي يكون وسيلة نشرة تقليدية مثل الصحف والمجلات، بينما الإعلان الإلكتروني تكون وسيلة نشره شبكة الإنترنت أو غيرها من الوسائل الإلكترونية الحديثة.

هذا وقد وجدنا التشابه واضحاً بين كلاً من التشريعين العربية في تحديد مفهوم المُعلن إلا أنهما لم يحددوا بشكل واضح وسائل الإعلان، مما قد يترتب عليه القول بان كلاً من المشرع الفلسطيني، واليمني، كذلك القطري، لم يضعوا النظام الإلكتروني كوسيلة من الوسائل المستخدمة حديثا للدعاية والإعلان، مما يجعلهم غير مدركين لمدى الخطورة التي قد يتعرض لها المستهلك الإلكتروني جراء تلك الإعلانات والوسائل الدعائية، وبخاصة إن كان الغرض منها ليس الربح وإنما كان غرض إجرامي.

[396] د/ نائل عبد الرحمن صالح، حماية المستهلك في التشريع الأردني، الطبعة الأولي، الأردن، مؤسسة زهران للنشر والتوزيع، 1991، ص 57. المزيد انظر: د/ هدى حامد قشقوش، الإعلانات غير المشروعة في نطاق القانون الجنائي، الطبعة الأولى، مصر، دار النهضة العربية 1998، ص 7.

[397] د/ هدى حامد قشقوش، الإعلانات غير المشروعة في نطاق القانون الجنائي، مرجع سابق، ص 4-5.

عند النظر جليا في التعريفات السابقة للمُعلن في قوانين حماية المستهلك، نجد أن هذه التعريفات جاءت مشابه إلي حد كبير للتعريف الوارد للمُعلن في قانون حماية المستهلك المصري رقم "181" لسنة 2018، إلا أن هناك اختلاف واضح بين تلك التشريعات فقد حرص المشرع المصري جعل الوسائل التي يستخدمها المعلن للإعلان عن السلع والخدمات غير محددة وقد ذكر صراحة علي الوسائل الإلكترونية، بهذا يكون قد شمل كل وسائل الدعاية والإعلان، حيث قد جاء باللائحة التنفيذية للقانون المشار إليه سابقاً، والتي قد جاءت واضحة في تحديد مفهوم المُعلن بأنه" كل شخص طبيعي أو اعتباري يقوم بالإعلان عن سلعة أو خدمة أو الترويج لها بذاته أو بواسطة غيره باستخدام أية وسيلة من الوسائل بما في ذلك الوسائل الإلكترونية وغير ذلك من وسائل التقنية الحديثة._ويعد معلنا طالب الإعلان، والوسيط الإعلاني، والوكالة الإعلانية، ووسيلة الإعلان، وذلك وفقا للمواصفات القياسية المصرية الخاصة باشتراطات الإعلان عن السلع والخدمات" كما ألزمت المعلن تجنب أى سلوك خادع فى الإعلان ذاته.[398]

وبالتالي فإن النص السابق يكون قد فتح المجال لدخول العديد من الطرق والأدوات الحديثة النابعة من التطور التكنولوجي ضمن وسائل الإعلان الواردة في نص قانون حماية المستهلك المصري.

بينما عرف المشرع المصري التسويق الالكتروني صراحة فى القانون رقم 151 لسنة 2020 على أنه" إرسال أي رسالة أو بيان أو محتوى إعلاني أو تسويقي بأي وسيلة تقنية أيا كانت طبيعتها أو صورتها تستهدف بشكل مباشر أو غير مباشر ترويج سلع أو خدمات أو التماسات أو طلبات تجارية أو سياسية أو اجتماعية أو خيرية موجهة الى أشخاص بعينهم.

هذا وتنقسم الإعلانات إلى أنواع مختلفة[399]، منها إعلانات موجهة للمستهلك حسب الهدف منها أو حسب المنطقة الجغرافية المراد التوزيع فيها، أو حسب نوعية النشاط الذي يمارسه المُعلن، أو حسب الأدوات المستخدمة، أو حسب السلع والخدمات محل الإعلان.

من التطبيقات الواقعية والعملية للإعلانات الإلكترونية، الإعلانات المنتشرة عبر الإنترنت، فعند القيام بفتح صفحة الإنترنت من خلال شاشة الكمبيوتر، تظهر بعض التبويبات للعديد من المواقع التجارية على صفحة الإنترنت، حيث يتم الدخول إلى أي عنوان من العناوين المعروضة بشكل مباشر، وتظهر هذه الإعلانات أعلي

[398] مادة 4، 5، 7،6، 8 من اللائحة التنفيذية للقانون رقم 181 لسنة 2018 بشأن حماية المستهلك الإلكتروني.

[399] د/ أسامه بدر، حماية المستهلك في التعاقد الإلكتروني، مرجع سابق، ص150.

صفحة محركات البحث (Yahoo, Google) بشكل عشوائي أو بمظهر ثابت، ومن الإعلانات الإلكترونية أيضا الرسائل القصيرة التي ترسل إلي الهواتف المحمولة للمستهلك أو إلي البريد الإلكتروني الخاص به ، وقد تكون الرسائل مصحوبة بالصوت والصورة.

وقد تناولت محكمة النقض الفرنسية الإعلان الإلكتروني حيث حددته بأنه "كل وسيلة معلوماتية تدفع العميل إلي تكوين عقيدة مقصودة من النتائج التي ستعود عليه من المال الذي سيشتريه أو الخدمة التي ستقدم له".[400]

والملاحظ من مقتضيات القانون التجاري و الجنائي المصري أنها لم تعط تعريفا للإعلانات الإلكترونية الخادعة والمضللة، بل عرفته اللائحة التنفيذية لقانون حماية المستهلك المصري رقم 181 لسنة 2018، نستخلص أن الإعلان الخادع هو ما اشتمل مضمونه على إدعاء أو بيان أو عرض كاذب أو يهدف إلى إيقاع المتعاقد في غلط، فالإعلان الذي يشتمل على إدعاء كاذب يعني استعمال ما من شأنه أن يجعل مضمونه إدعاءات مجردة عن الصحة، غايتها إيقاع المقصود بالإعلان في الغلط و إغرائه عن طريق ذلك من أجل استعمال السلعة أو الخدمة أو اقتنائها[401].

أما الإعلان الذي يشتمل على بيان كاذب يعني احتواء البيانات التي يرتكز عليها بشأن أحد العناصر المحددة على الكذب بغاية دفع الموجه إليه –المستهلك- إلى استهلاك السلع أو الخدمات أو اقتنائها، أما الإعلان الذي يشتمل على عرض كاذب يعني احتواء الإعلان على عرض السلع أو الخدمات لا يمت إلى الحقيقة بصلة في أي عنصر من العناصر الحقيقية الخاصة به. كما وقد حاول الفقه أن يقدم تعريفا للمصطلح فمنهم من ركز فقط على تعريف كلمة الخداع معتبرا بأنه إلباس أمر من الأمور مظهر يخالف حقيقة ما هو عليه، ومنهم من ركز على أشكال الإعلان الخادع كذلك الذي يحتوي على معلومات كاذبة، أو يتصف بالصدق والكذب الذي يتضمن معلومات غير كافية وبالمقابل هناك إحدى الآراء التي تعتبر بأن الإعلانات الخادعة هي التي يكون الغرض منها خداع المستهلك حتى و لو لم تكن في مضمونها كاذبة تماما[402].

---

[400] V,Cass. Crim. 12 november 1986, bull. Crim.p 261.

- مشار إليه لدى: د/أسامة أحمد بدر، حماية المستهلك في التعاقد الإلكتروني، مرجع سابق، ص 154.

[401] وفاء مصطفى محمد عثمان، توازن المصالح في تكوين عقد البيع الدولي للبضائع وفقا لاتفاقية فيينا لعام 1980، مرجع سابق، ص26 وما بعدها.

[402] د/ محمد نصر محمد القطرى، الحماية الجنائية من الخداع الإعلاني، مجلة الفكر الشرطي، مركز بحوث الشرطة، الشارقة، الإمارات العربية المتحدة، المجلد رقم 26، العدد 101، 2017، ص 224 وما بعدها. كذلك أنظر د/ أنطوان الناشف، الإعلانات والعلامات التجارية ، منشورات الحلبي الحقوقية، بيروت، 1999،ص9.

وعبارة الإعلان الخادع[403] تفرض تفكيكها لكي يفهم معناها بكيفية واضحة ذلك أن الإعلان أو الإشهار له معاني متعددة تتباين بحسب مجاله نقصره فقط على المجال التجاري الذي يقصد به لغة بأنه " النشاط أو الفن الذي يستهدف إحداث تأثير نفسي على المستهلك تحقيقا لغايات تجارية، ووفقا لذلك يراد به الوسيلة الفنية التي يستخدمها المعلن للتأثير النفسي و الذهني على المستهلك بقصد تحفيزه على شراء المنتج المعروض على احدى الصفحات الإعلانية على شبكة الإنترنت.

أما كلمة الخداع[404] فتتجه إلى تضليل المستهلك بإخفاء شيء هام عنه يتعلق بالمنتج سواء كان عمدا أو بطريقة الترك، و أيضا الكذب عليه و بهذا يكون خداع المستهلك مبنيا الكذب بتضمين بيانات أو ادعاءات مخالفة للحقيقة، ولذلك فإن الكذب هو أحد صور هذا الخداع على اعتبار أن الأساس في التعاملات الإلكترونية هو الثقة و الصدق و كلها صفات تتنافى مع الكذب الذي يمثل إدعاء وزعم مخالف للحقيقة شرط أن يرد كما جاء بالمادة 17 من اللائحة الخاصة بقانون حماية المستهلك المتعلقة بالسلعة أو الخدمة[405].

كما قد يكون خداع المستهلك مبنيا على التضليل و ذلك بصياغة عبارات تؤدي إلى خداعه أو بإخفاء شيء ما عنه و بهذا يقع الإعلان المضلل بين الإعلان الصادق و الإعلان الكاذب كونه لا يذكر بيانات كاذبة ولكنه يصاغ في عبارات تؤدي إلى خداع المتلقي، ومن ثم يستقيم مدلول الإعلان الخادع بكونه إخبار أو إعلان تجاري مظلل أو كاذب يسعى من ورائه المعلن إلى التعريف بمنتج ما كي يدفع بالمستهلك الإلكتروني إلى اقتنائه.

مما تقدم فإنه يمكننا لنا تعريف الإعلان الإلكتروني المضلل بأنه كلّ نشاط من شأنه أن يستخدم لترويج السلع والخدمات بأي وسيلة من وسائل الاتصال الحديثة بطريقة من شأنها تحفيز المستهلك الإلكتروني ودفعه إلى التعاقد لتحقيق مكسب مادي أو معنوي .

وما يؤيدنا في ذلك التعريف هو ما أولت به التشريعات القانونية اهتمامها في وضع تعريف للإعلان الإلكتروني المضلل ولعل القانون الفرنسي يعد في طليعة تلك القوانين، فقد عرفت المادة سالفة الذكر 121 من مدونة الاستهلاك الفرنسي رقم 939 لسنة 1993م الإعلان المضلل بأنه (كل إعلان يتضمن بأي شكل من

---

[403] د/عبد الله ذيب محمود، حماية المستهلك في التعاقد الإلكتروني، دراسة مقارنة، دار الثقافة، عمان، 2012، ص69.

[404] وفاء مصطفى محمد عثمان، توازن المصالح في تكوين عقد البيع الدولي للبضائع وفقا لاتفاقية فيينا لعام 1980، مرجع سابق، ص 26 وما بعدها.

[405] د/ محمد نصر محمد القطرى، الحماية الجنائية من الخداع الإعلاني، مرجع سابق، ص 235 وما بعدها. د/ فتيحة محمد قوراري، الحماية الجنائية للمستهلك من الإعلانات المضللة، مجلة الحقوق، كلية الحقوق، جامعة الكويت ، 2008.

الإشكال إدعاءات، أو إشارات أو تقديم خاطئ أو ذات طبيعة تؤدي إلى الوقوع في الخطأ عندما يتعلق الامر بواحد أو أكثر من العناصر الآتية , الوجود , الطبيعة , الصفات , التكوين , النوعية , العناصر الجوهرية, المصدر, الكمية, الطريقة وتاريخ الصنع , الثمن ، شروط البيع للسلع أو الخدمات, موضوع الإعلان, شروط الاستعمال النتائج المترتبة نتيجة الاستعمال , ودافع أو طرق البيع أو تقديم الخدمات ومضمون التعهد الذي يقوم به المعلن أو صفات أو قدرات المصنع ,البائع , المعلن أو مقدم الخدمات).

وبعد بيان موقف المشرع المصري فيما سبق فإننا نستنتج أن الإعلان الخادع يمكن تعريفة على أنه (كل سلوكا خادعا يتمثل في الفعل أو الامتناع عن فعل من جانب المورد أو المُعلن الذي يؤدي إلى خلق انطباع غير حقيقي أو مضلل لدى المستهلك أو يؤدي إلى وقوعه في غلط متى انصب السلوك على أي عنصر من العناصر المبينة في المادة (18) من اللائحة).[406]

إلا أنه هناك من العيوب التي اقترنت بالإعلان الإلكتروني مما جعل اثاره تأتي بالسلب لا بالإيجاب على المستهلك الإلكتروني ومن هذه العيوب:

1- عدم دقة بيانات الصلاحية للسلع.

2- عدم المقدرة على الحصول على تعويض في حال اكتشاف عيوب في السلعة خاصة إذا كان المنتج صنع في بلد آخر.

3- انعدام الصلة بين المصنع والمنتج والمستهلك وهذا الأمر يصعب على المستهلك إمكانية الرجوع في العقد أو المطالبة بالتعويض لا سيما في العقود ذات الطابع الدولي.

4- عدم وجود تباين في اللغات المستخدمة.

5- صعوبة قياس حجم السوق وذلك نتيجة عدم وضوح أدوات قياس واستنتاج عدد المستخدمين.

إلا ان ذلك لا يجعلنا ننكر الدور الهام والفعال للإعلان الإلكتروني الذي قد سهل الكثير من الوقت والجهد على المستهلكين عبر الإنترنت في الحصول على غالبية إن لم يكن كل السلع أو الخدمات التى يحتاجها المستهلك الإلكتروني، ولهذا يجب على الفقه والقانون والقــضاء، وبجانبهم العاملين في مجال حماية التقنية، أن يزيدوا من جهودهم المجدية في حماية المستهلك الإلكتروني من الإعلان المضلل وأشكاله وأساليبه.

[406] Cass .crim , 6 Mai 1998 , 26 Janv 1998 , 21mai 1984.

الفرع الثاني: شكل الإعلان الإلكتروني المضلل

إن بداية عرض السلع والخدمات عبر شبكة الإنترنت يكون عن طريق الإعلان عنها، فالإعلان هو من أهم الوسائل لجذب المستهلكين عبر شبكة الإنترنت وحمله على شراء السلع المعروضة و طلب الخدمات المختلفة عبر الإنترنت. وكما أوضحنا سابقا أن المقصود بالإعلان كل بيانات موجهة للجمهور من المُعلن بهدف جذبهم لطلب السلعة أو الخدمة المعروضة إلكترونيا.[407] وعليه فإن الإعلانات الإلكترونية التي تتم عبر شبكة الإنترنت لها وسائل متنوعة، منها ما يتم عرضة على صفحات الويب(Web)، أو ما يتم عرضه برسائل موجهة للبريد الإلكتروني للمستهلك، أو ما يتم من خلال ندوات الاتصال أو ما يسمى بمجالس النقاش أو بواسطة(Ftb)[408].

ولعل أكثر هذه الوسائل مشكلات قانونيـــة، الإعلانات الموجهـــة عبر البريد الإلكتروني. ففي هذا النطاق، فإن المادة العاشرة من الإرشاد الأوروبي الصادر بتاريخ 20 مايو 1997، المتعلـــق بالعقود المنشأة عن بعد، فيما يخص البريد الإلكتروني، بأنه لا يمكن استعمال تقنـــيات الاتصال عن بعد باتجاه المستهلك، إلا إذا غاب الاعتراض الواضح والصريح من جانبه من خلال رفض هذه الإعلانات، وخاصة عبر البريد الإلكتروني.[409]

وقد استقرت محكمة النقض المصرية مؤخرا على حجية المحررات الإلكترونية، وحجية البريد الإلكتروني، فالمشرع في المواد 1، 15 18 من القانون رقم 15 لسنة 2004، بشأن تنظيم التوقيع الإلكتروني...، كان حريصا على أن تتحقق حجية الإثبات المقررة للكتابة الالكترونية والمحررات الإلكترونية الرسمية او العرفية، من خلال حفظ الكتروني مستقل وغير خاضع لسيطرة منشئ هذه الكتابة او تلك المحررات، أو لسيطرة المعني بها...

وهو ما يدل على أن المشرع ارتأى مواكبة التطور التكنولوجي العالمي في المعاملات المدنية والتجارية والإدارية عن طريق تنظيمها ووضع ضوابط لها من أجل ترتيب آثارها القانونية......[410]

---

(407) J.Calais - Auloy, Frank Steinmetz: droit de La consommation, DALLOZ, 6ème, édition, 2003, p 132 n"125.

(408) (FTB): اختصار لـ File Transfer Protocol)

(409) د/ فريد منعم جبور، حماية المستهلك عبر الإنترنت، ومكافحة الجرائم الإلكترونية، دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الأولى،2010، ص 14.

(410) الطعن رقم 17689 لسنة 89 ق ، المستحدث، مكتب فني، جلسة 10 /2020/3.

لهذا فقد تم تفعيل نظام (L`opt-Out) الذي يلزم المستهلك بالاعتراض على الرسائل الإلكترونية التي لا يرغب فيها بعد وصولها إليه، وعلى عكس هذا النظام يوجد نظام آخر هو (L`opt - In) الذي يقتضي بموجبه الحصول علي رضاء المستهلك المسبق قبل إرسال الرسالة الإلكترونية إليه.

إلا أن الإرشاد الأوروبي السالف الذكر، قد أتاح للدول الأعضاء حرية وضـــع الأحكام القانونية الأكثر حماية للمستهلك، وقد استفادت بعض الدول الأوروبية من ذلك مــثل (النمسا، ألمانيا، الدنمارك، فنلندا، إيطاليا) ولجأت إلي إقرار نظام (L’opt - In) على أراضيها، إلا أن المشرع الفرنسي قد تبنـــى نظام L’opt - Out)[411].

هذا بجانب، أن بعض المُعلنين قد وضعوا نماذج للعقود والتي تتضمن نص يقضي بعدم اللجوء إلي إرسال الإعلانات الغير المرغوب بها من المستهلك، هذا وإن دل فإنه يدل على أنهم تبنوا نظام(L’op-In)، والجدير بالذكر أن كل نظام من الأنظمة السابقة له مبرراته التي تدعمه.

فنظام (Out- L’opt) يهدف إلى تفضيل مبدأ حرية التجارة وهو ما يسمح للمُعلن نشر إعلانه التجاري دون سبق موافقة من المستهلك أو المتلقي عن طريق هذا النظام يقوم المعلن بإرسال الإعلان الخاص به إلى الجمهور دون حاجة إلى موافقة مسبقة منهم، ومن مزايا هذا النظام أنه يساعد على ازدهار وتوسيع النشاط التجاري للمُعلن لما فيها من عرض السلعة بصورة مباشرة دون أي قيود تمنعه من إرسالها للجمهور، كما أن اعتراض المستهلك يأتي في مرحلة لاحقه لإرسال الإعلان وهذا يضمن للمُعلن التأكد من إطلاع المستهلك عليه مما قد يدفعه لشراء السلعة أو الخدمة المعروضة عبر شبكة الإنترنت.

أما نظام(in- L’opt) أكثر تشددا من النظام السابق عرضة، كما يعتبر قيد على مبدأ حرية التجارة، وأنه يدعم مبدأ تقيد التجارة لما فيه من جعل حماية المستهلك هي الأولوية القصوى على حرية التجارة، فيقوم هذا النظام على منع وصول الإعلانات إلى المستهلك دون موافقة مسبقة منه [412].

فالإعلان هنا يعد وسيلة لمساعدة المستهلك للحصول على السلع والخدمات المعروضة، كما يحقق له فرصة الاستعلام وحرية الاختيار من تلك السلع والخدمات المعروضة عليه عبر شبكة الإنترنت، على الرغم من

---

[411] **المادة L121-205 من قانون الاستهلاك الفرنسي.**

[412] **Mireille Antoine Et Co.: «Le Commerce Électronique Européen Sur Les Rails Cahiers Du Centre De Recherche Informatique Et Droits, Bruylant, Bruxelle, 2001).**

ذلك فقد يكون الإعلان خطر على حقوق المستهلك المحمية بموجب التشريعات المختلفة[413]، فقد يكون الإعلان خادعاً أو كاذبا، أو أنه لا يهدف إلي إيصال المعلومة الصحيحة وبصورة موضوعية وجدية إلي المستهلك.

وتعددت الطرق التي يستخدمها المعلنون لتضليل المستهلك الإلكتروني، سواء كان بوسيلة إيجابية أو بالترك وان كانت هي الأكثر شيوعا، فيعمد خلالها المعلن الى اغفال بعض البيانات الجوهرية فى التعاقد في التعاقد التى يرغب فى حث المستهلك عليها، فيضخم من مزايا التعاقد أو يخفي بعض التزاماته، وفي النهاية نجد ان التضليل له العديد من الصور والأشكال، فأي كانت هذه الطرق فإن الهدف منها تضليل المستهلك الإلكتروني والإعتداء على حقوقه[414].

المطلب الثاني: محل التضليل الاعلاني وضوابط حماية المستهلك الإلكتروني منه

بداية يعتبر الإعلان الموجة إلى المستهلك عبر شبكة الإنترنت دعوة للتعاقد أو دعوة للتفاوض، فلا يمكن اعتبار مجرد الإعلان إيجابا يلزم المُعلن بمجرد صدوره. عليه فإننا سوف نقسم هذا المطلب لفرعين أساسيين ندرس في الفرع الأول محل التضليل ، بينما نخصص الفرع الثاني لدراسة الضوابط القانونية لحماية المستهلك الإلكتروني من الإعلان المضلل في التشريع المقارن، وذلك تمهيدا لبحث أسس حماية المستهلك الإلكتروني من الإعلانات المضللة والخادعة بعد ذلك.

الفرع الأول: محل التضليل الإعلاني

إن أساليب التضليل الاعلاني لا يمكن حصرها، وإن كل محاولة لحصرها لهو أمر فى غير محله، ولكن ذلك لم يمنع الكثير من الأنظمة القانونية من تجريم الإعلانات المضللة لحماية المستهلك بصورة عامة سواء كان مستهلك تقليدي أو مستهلك إلكتروني، ولعل أول من سعى لتحديد هذه الأساليب هو المشرع الفرنسي فى المادة L 121-1 من قانون الاستهلاك الفرنسي، ونذكر من هذه الأساليب الآتي:

أولا: الخداع والتضليل الواقع على العناصر الذاتية للسلعة او الخدمة: فقد يرد الاعلان المضلل والكاذب على أحد العناصر الذاتية للسلعة أو الخدمة، فنجد أن الكذب هنا قد يقع على وجود السلعة او الخدمة نفسها، سواء كان في انها غير موجودة أصلا، أو أنها موجودة ولكن غير مطابقة لما تم الاعلان عنه، او انها غير معدة

[413] د/ فريد منعم جبور،حماية المستهلك عبر الإنترنت، مرجع سابق، ص15.

[414] د/ محمد نصر محمد القطرى، الحماية الجنائية من الخداع الإعلاني، مرجع سابق، ص 240 وما بعدها.

للتسليم، كما قد يرد الإعلان المضلل على وجود الخدمة سواء ان المعلن غير قادر على تقديمها بالكيفية المعلن عنها إلكترونيا .[415]

وينكشف عن ذلك الادعاء وجود سلعة أو تقديم خدمة غير متوفرة علي الإطلاق، أو موجودة ولكن بصورة غير المُعلن عنها أو الموجودة، ولكن بشكل غير معد للتسليم، فهناك ثلاث أشكال تتعلق بالإعـــلام الكاذب والمضلل في وصفه:

1- الشكل الأول: أن يعلن المنتج أو البائع عن وجود سلعة من ماركة معروفة[416]، وهي غير موجودة أصلاً أو موجودة ولكن من نوعية أقل.[417]

2- الشكل الثاني: قيام أحد التجار عن بيع محمول من نوع غالي الثمن مع قرين بالحجز في أحد الغرف في فندق بقرية سياحية ، ويتضح أن هذه القرية في مرحلة الإنشاء ولم تنتهي بعد.

3- الشكل الثالث: أن يقوم أحد التجار بالإعلان عن بيع أراضي يتم تسليمها فور التوقيع على العقد، بينما احتوت المستندات على العديد من الشروط لم تكن وقت الرسالة الإعلانية قد تحققت[418] .

وقد قضت محكمة شمال القاهرة الاقتصادية حكما بتغريم شركة راية مبلغ 5000 جنيهاً، مع إلزام الرئيسة التنفيذية للشركة بنشر الحكم في جريدتين واسعة الانتشار بسبب إعلان الشركة عن شراء هاتف محمول مع الحصول على أربع ليالي بأحد الفنادق، ولكنها لن تنفذ العرض الذي تضمنه الإعلان[419].

ثانيا: الخداع الإعلاني فى طبيعة السلعة أو الخدمة: تظهر خطورة هذه الطريقة فى ان التغير لا ينصب على الاعلان ذاته او الخدمة ذاته وانما ينصب الخداع هنا على جوهر الخدمة أو السلعة المعروضة إلكترونيا[420].

---

(415) د/ محمد نصر محمد القطرى، الحماية الجنائية من الخداع الإعلاني، مرجع سابق، ص 259 - 260.

(416) Appel, Lyon 5 Mai 1983 : J.C.P. 1989 11970 Note Bidag (J.J).

(417) Cass. Crim. 3 Janu. 1984 : J.C.P 1984 Ivp. 772 Juin 1982 : Revu. Trim. Dr. com 1983. P 292 Obs. Bosât.

(418) Crime, 8 nov. 1983, (D. 1984 I.R.P. 59.

(419) تم إنشاء المحاكم الاقتصادية بالقانون رقم 120 لسنة 2008 وتم نشره بالجريدة الرسمية بتاريخ 22 مايو 2008 يتكون من 6 مواد إصدار ويليها مادة وعمل بها في أكتوبر 2008 " والملاحظ أن اختصاص المحكمة الاقتصادية أخضع في تطبيقات العقوبات للمحكمة الاقتصادية دون غيرها ولكن لم يخضع حماية المستهلك في شقها المدني. وهذا تناقض غريب لأنه يجب أن تكون حماية المستهلك جزء واحد لا يتجزأ.

(420) د/ محمد نصر محمد القطرى، الحماية الجنائية من الخداع الإعلاني، مرجع سابق، ص 261. د/ فتيحة محمد قوراري، الحماية الجنائية للمستهلك من الإعلانات المضللة، مرجع سابق.

ويتعلق الخداع في هذه الصورة بطبيعة المنتج أو الخدمة محل الإعلان، الأمر الذي يجعله يتحول إلي شيء ذي طبيعة أخرى، وتكمن خطورة الإعلان التـــجاري الكاذب في هذه الحالة أن إقـــبال المستهلك علي التعاقد بشأن السلعة أو الخدمة محل الإعلان إنما يرد علي سلعة أو خدمة مخالفة للحقيقة، الأمر الذي قد يضر المستهلك بأضراراً بالغة[421] .

وأكد القضاء الفرنسي علي هذا في أحكامه حيث ذهب إلي أن الخداع في طبيعة المنتج أو الخدمة يشكل منافسة غير مشروعة من جانب المعلن، فإذا ما فقدت السلعة أو الخدمة طبيعتها الحقيقة التي تكسبها جوهرها الحقيقي يعد ذلك تضليلاً للمستهلك وخداعاً له. ومثال على ذلك :

إذا قضي في جنحة إعلان خادع بالحكم على المعلن لإعلانه عن تحفة من البرونز مع إنها من معدن أقل قيمة والإعلان عن قماش من القطن مع أنها من ألياف صناعية أقل جودة.. الخ.

ثالثا: وقوع الخداع على أصل المنتج او الخدمة او المصدر: هذه الصورة من الخداع تؤثر على القناعة الشخصية للمستهلك الإلكتروني، وهذا ما يبرز خطورتها، في أنها تمثل تغير في الأصل أو المصدر الحقيقي للمنتج نفسه، فمن يعلن عن كلب رومي صغير في حين أنه ليس كذلك، فإن ذلك يعد من قبيل الإعلان الخادع[422].

فالعديد من المستهلكين يرتبط في أذهانهم عناصر الجودة بأصل المنتج أو الخدمة، لذلك عبر القضاء الفرنسي أن الإعلان يكون خادع وبشكل منافسة غير مشروعة عندما يشير إلي أصل المنتج أو الخدمة محل الإعلان علي خلاف الحقيقة ؛ لأنه عندما يتخذ المستهلك قرار بشراء سلعة أو الحصول علي الخدمة، فإنه يكون مدفوعاً إلي أصل السلعة ومصدرها.

رابعا: وقوع الخداع على الخصائص الجوهرية للسلعة او الخدمة: الخداع والتضليل في هذه الحالة يتعلق بالصفات الجوهرية للمنتج أو الخدمة محل الإعلان، وهي التي يضعها الشخص في الاعتبار عند التعاقد علي

([421]) د/ سيد محمد سيد شعراوي، الحماية المدنية للمستهلك في عقود البيع الإلكترونية، جامعة عين شمس، 2010، ص157.

([422]) د/ محمد نصر محمد القطرى، الحماية الجنائية من الخداع الإعلاني، مرجع سابق، ص 262 وما بعدها. كما أنظر في ذلك د/ محمد ابراهيم السحيباني، السلع المعلوماتية، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة 1:3 / 5/ 2000، المجلد الأول، الطبعة الثالثة، 2004، ص 263 وما بعدها.

المنتج أو الخدمة، وهي مسألة تقديرية تختلف بإختلاف الأشخاص والعقود والأشياء الدافعة للتعاقد[423]، وقد جاء ذلك مطابقاً للتوجيهات الأوربية بشأن الإعلان الكاذب والمضلل عام 1984، 1997، 2005، 2006 ، وقد تركت تلك التوجيهات للدول الأعضاء تحديد العقوبة.

وتطبيقاً لذلك حكمت الدائرة الجنائية لمحكمة النقض الفرنسية بجلسة 2 أكتوبر 1996 في سند الدعوى المقامة من شركة تعمل في مستشفيات صمغ الصنوبر، وتتلخص وقائع القضية في قيام شركة سان مارك بالإعلان عن بيع سائل منظف أطلقت عليه أسم (صنوبر لاند)، وذلك نسبة إلي أنه داخل في تكوينه مادة فعالة من مستخلصات نبات الصنوبر سبق زراعته في منطقة رملية كانت قد زودتها بها شركة لمشتقات صمغ الصنوبر، وقد تتضمن الإعلان أن جودة هذا المنتج في رائحته وعطرة الطبيعي بإعتبار أن ذلك يمثل إحدى الصفات الجوهرية للمنتج.

وعقب ذلك أعلنت شركة Benkiser عن وجود منتج مماثل، وأطلقت عليه نفس الاسم التجاري له إلا أنها اكتفت في مجال التفرقة بينهما إلي أنه عامل معطر فقط، فتقدمت الشركة الأولي بشكوى وادعت بالحق المدني أمام قاضي التحقيق منددة بإستخدام إسم صنوبر لاند، حيث أحيل مديرو الشركة الثانية إلي محكمة الجنح لاتهامهم بنشر إعلان من شأنه التضليل فيما يتعلق بالصفات الجوهرية للمنتج، وقد تمسك المدعي عليهم بأن الفعل المجرم ليس خاطئاً، إذ أنه ليس من شأنه تضليل المستهلك بخصوص أحد العناصر المشار إليها في المادة (L-121-1) من قانون الاستهلاك الفرنسي عام 1993.

وفي هذا الصدد يمكن القول أن الجمهور يستطيـــع أن يستشعر الإعلان الكاذب للسلعـــة أو الخدمة كونها صفة جوهرية عند القيام بالشـــراء، وقد أكدت محكمة النقض الفرنسية ذلك حيث أشارت إلي أن جوهـــر الشـــيء لا يقتصر على ما ينسبه إليه المستهلك كصفـــة، بل هو أمر متعلق بتكويـــن المنتج نفسه، وأن المستهلكين الذين كانوا يستخدمـــون منتـــج الشركة الأولي كانوا يعرفـــون أن الرائحة تُعـــرب عن تركيب حقيقي أو طبيعي، في حين أن الشركة الثانية تقدم لهم رائحة دون أن يتوافر لها طبيعة التركيب نفسها.[424]

[423] د/ عبد الفضيل محمد احمد، الإعلان عن المنتجات والخدمات من الوجهة القانونية، مكتبة الجلاء الجديدة، المنصورة، 1992، بند 4، ص 35. محمد احمد ابو الهنا، مرجع سابق، 173.

[424] Cass Crim. 15 Mai 2001 : J.C.P 2001, ed E.P. 136 : Cass Crime 19 Nov. 1991. Desponsible. Sur.www.legifrnce.com

خامساً: مقدار البضاعة : إذا انطوى الإعلان التجاري علي خداع أو تضليل حول الكمية أو المقدار الحقيقي للمنتج أو الخدمة محل الإعلان يعد كاذباً، وهنا يجب علي المحكمة أن توازن بين الكمية أو العدد أو الوزن أو المقاس الوارد في الرسالة الإعلانية، وما تم تسليمه بالفعل للمستهلك، فإذا كان الفارق بينهما مما لا يجري العرف أو العادة علي التسامح فيه كنا بصدد إعلان تجاري كاذب ومثال علي ذلك: قضي بأن الإعلان يكون خادعاً إذا كانت هناك مبالغة كبيرة في مساحة الشقة المعروضة للبيع، وكذلك يُعد إعلاناً خادعاً قيام وكالة للتأجير العقاري بنشر قوائم لشقق مع العلم بحظر التصرف فيها.

ويُعد أيضاً إعلاناً كذاباً وخادعاً إذا عرض سلعة على أن وزنها 350 جرام، ولكنها في الحقيقة لا تتعدى 250 جرام، وأيضاً إعلاناً أحدي الوكالات العقارية عن بيع أرض فضاء صالحة للبناء، مساحتها 3000 متر مربع، والحقيقة أنها 2556 متر مربع فقط.

سادساً : مكونات المنتج أو الخدمة : يأخذ الكذب في الإعلان التجاري فيما يتعلق بهذا العنصر إحدى الصورتين: الأولي الإعلان عن مكونات السلعة غير موجودة على الإطلاق، والثانية الإعلان عن مكونات لسلعة موجودة بالفعل ولكن بنسبة غير المعلن عنها.

ولذلك قضي بأن الإعلان عن منتج لمعالجة سقوط الشعر زعم المعلن كذباً بأنه يحتوي علي بروتينات ومستخرجات للغدد يعد إعلاناً خادعاً.

أيضا يُعد إعلاناً خادعاً ذلك الذي يعلن عن معجون أسنان يحتوي على نوع من الفيتامينات، وينصح أنه على خلاف الحقيقة.

ثامنا: الخداع الوارد فى عناصر السلعة او الخدمة الخارجية: إن الكذب بشأن العناصر الخارجية عن المنتج أو الخدمة يعد غير مشروع، لأن هذه العناصر تمثل إعتبارات معينة تحيط بالمنتج محل الإعلان دون أن تتعلق بذاتية أو خصائص المنتج الداخلية، وهذه العناصر كما ورد النص عليها في القانون الفرنسي المادة 44 من القانون رقم 73-1193 الصادر فى 27 ديسمبر 1973 بشأن التجارة والصناعة التقليدية هي طريقة ، وتاريخ الإنتاج ، وثمن البضاعة، وشروط البيع، والأثر الفعال للسلعة، والنتائج المتوقع الحصول عليها من السلعة، والباعث وإجراءات البيع، والصفات الجوهرية. [425]

---

[425] **Loi n°(73-1193) du 27 décembre 1973 d'orientation du commerce et de l'artisanat Titre III : Dispositions économiques Chapitre III : Amélioration des conditions de la concurrence.**

1- الكذب بشأن طريقة الصنع وتاريخ الإنتاج: يُعد الإعلان غير مشروع عندما يتضمن تضليلاً أو خداعاً للمستهلك حول طريقة تصنيع المنتج محل الإعلان، كأن يذكر في الرسالة الإعلانية أن الفطائر المعروضة للبيع مصنوعة بالمنزل مع أنها مصنعة آلياً، الأغذية التي تقدم عادة في الإعلانات على أنها طازجة، بينما الحقيقة على خلاف ذلك كما هو الحال في الشعارات الإعلانية الخاصة بالخبز الناضج علي نار من الخشب مثلاً.

2- الكذب بشأن ثمـن البضاعة: إن الكذب والتضليل فيما يتعلق بسعر السلعة أو الخدمة يتميز عن باقي صفوف الكذب،لأن بمقتضى السعر غالباً يحدد المستهلك قراره بالشراء.

ولذلك يُعد الإعلان غير مشروع عندما يتضمن تضليلاً أو خداعاً للمستهلك حول السعر، لأنه يؤدي إلي جذب المستهلكين إلي مكان البيع مدفوعين بالوهم الذي أنماه في داخلهم، وفي هذه اللحظة يتفاجأ المستهلك أن الثمن الذي أعُلن عنه غير حقيقي.

وقد أوردت المادة (L-121-1) من مدونة الاستهلاك الفرنسي الصادرة عام 1993 أن الثمن من ضمن العناصر التي يقع عليها الكذب والتضليل.

مما هو جدير بالذكر أيضا أن الكذب والخداع يتحقق عندما يشير الإعلان إلي وجود تخفيضات في الأسعار على المنتجات بنسبة 25٪، في حين أن هذا التخفيض لا يشمل إلا جزءاً من المنتجات التي لا تتعدى نسبة التخفيض فيها 20٪، وعلى ذلك استقر القضاء الفرنسي علي أن أي كذب أو تضليل للمستهلك في الإعلان عن أثمان المنتجات أو الخدمات يعد عملاً غير مشروع،لأنه ينطوي علي خداع المستهلك.

وقد استقر القضاء الفرنسي على أن كل تاجر من حقه أن يضع الأسعار التي يراها بما لا يعد خروجاً على قواعد المنافسة المشروعة، وله أن يتبع وسائل المضاربة المشروعة في تسعير منتجاته وخدماته، ولكن عليه أن يلتزم بما أعلن عنه من أسعار سواء أكان في إعلاناته خارجية أو داخل المحل أو على المنتجات.

3: الكذب بشأن شــروط البيع : أضيفت صورة الكذب والخداع إلي نص المادة 44 من القانون رقم 73-1193 الصادر فى 27 ديسمبر 1973 ، وذلك لمواجهة الفروض التي يعمل فيها المعلن على جذب العملاء بالإعلان كذباً عن شروط ميسرة للبيع ، فالخداع والتضليل حول شروط البيع يُعتبر عملاً غير مشروع. والإعلان عن

ضمان المبيع لمدة عشر سنوات بينما الحقيقة أنه مضموناً لمدة 3 سنوات فقط، والإعلان عن البيع بالتقسيط، بينما الحقيقة أنه يشترط سداد ثلث الثمن أو 30٪ من الثمن قبل التسليم[426].

4: الكذب بشأن الأثر الفعال "للسلعة أو المنتج": الأثر الفعال للمنتج هو أن تحتوي السلعة على خاصية ما أو على أثر ما وهو كما عبر عنه البعض[427] يكتنفه الغموض، وذلك لأن الأثر إما يتعلق بالخصائص الجوهرية للمنتج أو أن يدخل ضمن مكونات المنتج، وهو الذي نص عليه المشرع عندما أشار إلي العناصر الذاتية للمنتج أو الخدمة وتكرار ذلك. والسؤال الذي يضع نفسه هو ما مغزي إضافة هذه الحالة ضمن محل الكذب والتضليل في الإعلانات التجارية؟

والواقع أن المشرع لم يقصد عندما نص على تحريم الرسالة الإعلانية التي تحتوي على وقائع كاذبة أو مضللة، خاصة بالأثر الفعال للمنتج وإنما أراد أن يواجه الحالة التي ينصب فيها الكذب والتضليل على الأثر الفعال لمنتجات معينة كالمنتجات الصيدلانية أو منتجات التجميل أو النظافة لما لها من أثر خطير علي صحة المستهلك. لذلك حكمت محكمة استئناف بحكمها الصادر في 5 ديسمبر 1997[428] أن الإعلانات التجارية التي تعلن عن إنقاص الوزن الزائد في منطقتي البطن والأرداف، وذلك ومن إتباع أي حمية أو نظام غذائي أو علاجي فقط ارتداء حذاء يستخدم أثناء السير رغم الإشارة من بعض الأطباء بفاعلية وصلاحية المنتج في إنقاص الوزن الزائد، إلا أن المحكمة اعتبرت هذا هو الصحيح أن هذا التقرير ليس له صفة رسمية.

وكثرت هذه الأنواع من الإعلانات مثل الأقراص والكريمات التي تقوم بالتحصين وأدانت المحكمة هذه الأنواع من الإعلانات أيضا. ولكن في بعض البلاد لم تصل إلي تجريم هذا النوع حتى الآن، وتكثر فيها الكذب والتضليل في إعلاناتها التجارية نظرا لعدم وجود نص خاص وصريح يحرم الدعاية الكاذبة والمضللة، إذا انصبت علي الأثر الفعال للسلعة أو المنتج، وختمت المحكمة وأنهته إلي أنه يجب على المعلن إثبات صحة الادعاءات التي تضمنتها الرسالة الإعلانية، فضلاً عن ضرورة مساندة أقـوال المعلن ببراهين علمية وأختبارات صادقة[429].

---

[426] د/ خالد عبد المنعم إبراهيم مصطفى، حماية المستهلك في التعاقد الإلكتروني، مرجع سابق، ص 318.

[427] د/ محمد أحمد أبو الهنا، مرجع سابق، ص 179. وقد أشار الى، د/ أحمد السعيد الزقرد، الحمايه المدنيه من الدعاية التجارية الكاذبة والمضللة ، مرجع سابق، ص113.

[428] محمد احمد ابو الهنا، مرجع سابق، ص 180.

[429] C.A Paris 5 Déc, 1997, Conçu. On cède. Juris la sseeur. N 11 Nov. 1998 com. Ment A n° 154. Publicité Trompeuse, P2012.

5- الكذب بشأن النتائج المتوقع الحصول عليها من السلعة أو المنتج : أعتبرت المحاكم الفرنسية من قبيل الإعلان الكاذب والخادع إعلان صاحب محل تصوير انه يكبر الصور الفوتوغرافية إلي حجم 2.25 متر وأكثر خلافاً للحقيقة[430]، أيضاً الإعلان كذباً عن نوع من العقاقير الذي يسبب النحافة. والإعلان كذباً عن نوع من المشروبات التي يدعي أنها تتضمن علي عناصر تضمن للشخص حيوية دائمة غير عادية، وغيرها من الإعلانات التي تتضمن على كذب يقع علي النتائج المتوقعة من السلعة أو المنتج.

6- الخداع الذي يؤثر على دافع المستهلك الإلكتروني وإجراءات البيع: في هذا السياق أدانت محكمة استئناف (بواتييه) بجلستها المنعقدة في 15 نوفمبر 1990 المعلن عن بيع ملابس في مقر شركة تعمل في مجال التصفيات الفضائية بتهمة الإعلان الكاذب، حيث أفسح المجال للإعتقاد بأن البضاعة المعروضة واردة من مخزن هذه الشركة، وذلك أن المستهلكين يكونوا أكثر حساسية بالنسبة للعروض الخاصة بالتخفيضات بصفة عامة، وتخفيضات أسعار الملابس بصفة خاصة.[431]

وعلي نفس النهج قيام صاحب محل تجاري بالإعلان أنه:(بعد 75 سنة من العمل يقرر المحل إغلاق أبوابه مضطراً وتصفية كل مخزونه من الملابس مضحياً بها بأسعار منخفضة لظروف الاستعجال[432]، ورغم ذلك حكم عليه بالبراءة، رغم أنه أوهم جمهور المستهلكين بوجود صفقة وفرصة لن تتكرر وهي التصفية بأسعار مخفضة[433].

فالإعلان إذا كان غير واضح وغير محدد فيما يتعلق بالدافع من وراء عرض السلعة أو الخدمة فإنه يكون خادع ومضلل وكاذب، وبالتالي يعتبر عملاً غير مشروع وإعلان تجاري غير نزيه يسأل عنه المعلن الذي يشير علي غير الحقيقة.

7 - خداع المُعلن المستهلك الإلكتروني ضمانات ما بعد البيع : قد تكون تعهدات المعلن التي قطعها علي نفسه أو أعلن عنها التي دفعت المستهلك بإتخاذ قراره بشراء سلعة أو التعاقد علي خدمة مدفوعة بهذا التعهد، وإذا اثبت فيما بعد عدم صدق هذه التعهدات، فإن ذلك يمثل خداعاً وغشاً للمستهلك، لذا صرحت معظم

---

[430] T.G.I. Seine . 4 Juillet 1968. "Grossit des photos jusqu'à une hauteur de 2.50m. du plancher et Jusqú au plafond si vous le désirez".

[431] C.A Poitiers, 15 Juin 1990, Rev. Dr. Pén. 10 année hors série déc 1998, P. 91.

[432] Rouen 14 février 1975: D. 1975. 363 : Zomai 1975. D. 1976 52:R.T.D Comme 1976 - P.426, N °.

[433] د/ أحمد السعيد الزقرد، الحمايه المدنيه من الدعاية التجارية الكاذبة والمضللة ، مرجع سابق، ص 118.

النصوص القانونية علي تحريم الرسالة الإعلانية التي ينصب فيها الكذب أو التضليل على مضمون مغزى متعهدات المعلن.

ويتضح هذا بشكل أساسي في الإعلانات عن خدمات ما بعد البيع أو ضمان قطع الغيار للماكينات أو الأجهزة المعلن عنها. وهكذا فإن البائع الذي يعلن كذباً أن كل مبيعاته يمكن تغييرها أو استبدالها بغيرها بشرط أن تكون بحالة جيدة ويخل بهذه التعهدات يقع تحت طائلة القانون[434].

فأي خداع أو تضليل للمستهلك بشأن تلك التعهدات يؤدي إلي إنعقاد المسئولية عن الأضرار التي تلحق بالمستهلك، ويحدث هذا الخداع عندما يتعهد المعلن بالتزامات في رسالة إعلانية لا يستطيع الإلتزام بها وتنفيذها أو يقوم بتنفيذ إلتزامات أخري بديلة عنها.

الفرع الثاني: الضوابط القانونية لحماية المستهلك الإلكتروني من الإعلان المضلل في التشريع المقارن

بعد عرض الطبيعة القانونية للإعلان الإلكتروني، يجب أن نوضح مدى خطورة الإعلان على حقــوق المستهلك الإلكتـروني بصفة خاصـة، وهذا ما دعي المشــــرع في الكثـير من الدول إلى التدخــل ووضع ضوابط قانونيـــة ملزمة ومقترنة بجـزاءات جنائية قد تكون رادعــة، لمنع الإعــلانات الخادعة والكاذبة، ومحاربة صـور التضليل الإلكتروني التي قد يقــع المستهلك فريسة لها سواء كان ذلك على المستوى الوطني أو المستــوى الدولي.

حتى أنه لتفادى مخاطر الإعلانات الإلكترونية المخادعة، ولكي لا تتزعزع المستهلك الإلكتروني بالمُعلن والسلع والخدمات التي يعرضها، قد وضع المُعلنين في بعض الدول مجموعة من الضوابط للتنظيم الذاتي للإعلان وألزموا أنفسهم بها، جاعلين الهدف الأساسي من هذا التنظيم هو طمأنينة المستهلك الإلكتروني، وحتى يؤدي الإعلان هدفه ووظيفته في جذب وإعلام المستهلك بالسلعة أو الخدمة المعروضة، وهو أمر لجأت إليه أيضا غرفة التجارة الدولية بباريس، واضعة تنظيما للسلوك المحلي بمادة الإعلان، أوضحت فيه المبادئ الأخلاقية لمهنة الإعلان التي يجب على المُعلنين الالتزام بها، كما ذهب المحترفون في بعض البلدان مثل فرنسا إلي إيجاد مكتب للتحقق الإعلاني(BVP)[435] ، وقد جاء تنظيم أخلاقيات مهنه الإعلان، مطابقا للغاية

---

[434] C.A. Aix – en Provence, 16 Juin. 1965, cite par. P.et.F. greffe. N 1109. P.339.

[435] BVP اختصار لـ : (le bureau de verification de la publicité)

التي تبنتها غرفة التجارة الدولية بباريس السابق ذكرها، حيث كان الهدف من وضع تلك الأخلاقيات هو ضمان التزام واحترام الأعضاء والمنتسبين الجدد لها بتلك الأخلاقيات المتبناة من قبلها[436].

إلا أن ذلك يحل محل تدخل المشرع والمحاكم في وضع الضوابط القانونية والنصوص التشريعية الملزمة والمقترنة بجزاءات جناية تضمن الالتزام بها وتوقع على من يخالفها، لمواجهة خطورة ما يتعرض له المستهلك الإلكتروني من الإعلانات، ويبقى السؤال المطروح هنا ما هو محتوى الضوابط والأحكام التي يجب على المعلن الالتزام بها حتى يكون إعلانه داخل إطار قانوني صحيح؟

إن الإجابة على هذا التساؤل تستلزم منا عرض مضمون هذه الأحكام على المستوى الأوربي، كما على مستوى التشريع الفرنسي باعتباره كان سباقاً في التنبه لهذه المعضلة، ثم نوضح ما تضمنته بعض التشريعات العربية من ضوابط وأحكام ونختمها بموقف المشرع المصري من تلك التشريعات.

أولا: موضوع الإعلان على المستوى الأوروبي: نجد في هذا الاتجاه العديد من التوجيهات والإرشادات الأوروبي والتي تبنت موضوع الإعلان ومواجهة الإعلان الكاذب والخادع، ومنها الإرشاد الأوروبي المتعلق بالإعلان الخادع والإعلان المقارن لعام 1997[437].

كما أن الإرشاد الأوروبي الخاص بالتجارة الإلكترونية عام 2000 (رقم 31/2000 تاريخ 8 يونيو 2000)، وأيضا ما يسمى بالكتاب الأخضر (LIVRE VERT) الصادر عن اللجنة الأوروبية منذ عام 1996[438]. وملحقه الصادر بتاريخ 4 مارس 1998. هذه النصوص ذات التوجه العام، التي تطبق بصورة أولي على الإعلان الخادع المنشور على شبكة الإنترنت، قد حددت مفهوم الإعلان بأنه يشمل أي شكل من أشكال الاتصال في إطار النشاط التجاري والصناعي والحرفي والمهن الحرة, وذلك بغاية تسويق البضائع والخدمات بما فيه الأموال غير المنقولة، والحقوق، والواجبات[439].

---

[436] د/ فريد منعم جبور، حماية المستهلك الإلكتروني عبر الإنترنت، مرجع سابق، ص 16. د/ محمد نصر محمد القطرى، الحماية الجنائية من الخداع الإعلاني، مرجع سابق، ص 246 وما بعدها. د/ فتيحة محمد قوراري، الحماية الجنائية للمستهلك من الإعلانات المضللة، مرجع سابق.

[437] **(Cons. Ue, dir. n'' 97 / 55 / CE, 6 Oct. 1997, mod. Dir n'' 84 / 450 / CEE).**

[438] **(Livre vert de la commission européenne: «les communications commerciales dans le marché intérieur». 8 mai 1996: Doc. Com (1996), 192 final).**

[439] **د/ هدى حامد قشقوش، الإعلانات غير المشروعة في نطاق القانون الجنائي، مرجع سابق، ص 38.**

ثانيا: موضوع الإعلان في التشريع الفرنسي : لم يضع التشريع الفرنسي تحديدا معيناً للإعلان بصورة مباشرة، بل منع في المادةL(1-121)[440] وما يليها من قانون الاستهلاك، الإعلان الخادع الذي يتم بأي شكل من الأشكال، ويشتمل على: بيانات أو عروض كاذبة أو تلك التي من شأنها أن تؤدي إلي الخداع أو التضليل، ويقع علي عنصر أو أكثر من عناصر السلعة أو الخدمة وخاصة منها التالية: الوجود (l'existence)، الطبيعة، التركيب، الصفات الجوهرية، المصدر، النوعية، الكمية، الشكل وتاريخ الصنع، الخواص، السعر، شروط الاستعمال ومحاذيره، شروط البيع، الفوائد، مدى التزامات المعلن... الخ. كما أن نص المواد L121-2 إلي L121-7 من قانون الاستهلاك الفرنسي تفترض وجود ثلاث شروط مجتمعة حتى يمكن اعتبار الإعلان الإلكتروني جريمة هي :

الشرط الأول: أن يكون هنا إعلان فعلي مهما اختلفت وسيلة نشرة (شبكة الإنترنيت – راديو – لوحة إعلان – تلفزيون..) أو مهما اختلف شكل الإعلان (كلمات – صور – حديث – بيانات..) أو تنوعت السلعة أو الخدمة أموال غير منقولة – منقولات – خدمات...) أو أيا كانت صفة المُعلن فقد يكون محترفا أو غير محترف وقد يكون شخصا طبيعيا أو معنويا.

الشرط الثاني: أن يكون هناك خداع حتى ولو لم يؤد فعلا إلي إيقاع المستهلك الإلكتروني في الخطأ[441].

الشرط الثالث: أن يكون الخداع على أحد العناصر المذكورة في نـص المادة(L121-1) المذكورة سابقاً [442].

نستخلص من ذلك أن جريمة الإعلان الخادع كما جاءت في قانون الاستهلاك تقع حتى وإذا لم يكن هناك سوء نية من جانب المُعلن، حيث أن جريمة الإعلان الخادع هي جريمة مادية ، تقوم على مجرد الإهمال أو عدم الاحتراز عند نشر الإعلان على شبكة الإنترنت أو على أي وسيط إلكتروني أخر.

ثالثا: موضوع الإعلان المضلل في القضاء الفرنسي:- أقر القضاء الفرنسي بأن الإعلان المضلل هو كل ما يوقع المستهلك في غلط[443]، فإن هذه التوليفة، المتعلقة بالجنحة المنصوص عليها في المادة 121-1 من تقنين

---

[440] (Art L122-1 (code de consommation) «est interdite toute publicité comportant, sous quelque forme que ce soit, des allégations, indications ou présentations fausses ou de nature à induire en erreur, lorsque celles-ci porte sur un ou plusieurs des éléments ci après:

[441] J. Calais - Auloy et F. Steinmetz: " droit de la consommation" op. cit. P 140.

[442] Y. Picod et H. Davo: " droit de la consommation", éd DALLOZ, 2005, P 72.

[443] A. Giudicelli, Chroniques, Rev. Sc. Crim., 1999, P.115

الاستهلاك، ترتكز على ما يزيد عن الثلاثين حكماً قضائياً صادر بطريق محكمة النقض، والمحاكم الأدنى درجة، خلال الفترة التي تمتد من أكتوبر 1997 وحتى سبتمبر 1998. ومن خلال هذه الأحكام المتنوعة سوف نرصد على وجه الخصوص، تلك التي صدرت في شأن الإعلان المضلل.

بداية، وفيما يتعلق بالجانب النفسي لمرتكب الجريمة، فقد أكد العديد من الأحكام القضائية على أن الخطأ، أو الإهمال يكفي لإسناد التهمة، "وسوء نية المعلن لا يعتبر ركن في جنحة الإعلان الكاذب، أو الذي يؤدي بطبيعته إلي الوقوع في الخطأ[444]". وعلى الرغم من أن بعض الأحكام لم تألوا جهداً في سبيل تمييز القصد الجنائي[445]، إلا أن خطأ الفاعل يمكن استنباطه من مجرد المعرفة البسيطة بعدم صحة البيانات الواردة في الإعلان، وعدم تحري الدقة والسلامة في المعلومات التي ينقلها إلي الجمهور[446].

وعلى نحو ما سبق وأن أشرنا أنفاً، إن جنحة الإعلان الكاذب، أو الذي يؤدي بطبيعته إلي الوقوع في الخطأ تبدو كما لو كانت جنحة متلونة **un délit caméléon**، إذ من الممكن أن يتنوع الجانب النفسي لها، على الرغم من ضرورة، وكفاية في ذات الوقت إثبات الإهمال، أو الخطأ.

بينما وفيما يتعلق بالركن المادي للجريمة، فإن العديد من الأحكام القضائية تشهد على اتجاه القضاء نحو الأخذ بالتفسير الواسع لفكرة الإعلان، المنصوص عليها في المادة 1121-1 من تقنين الاستهلاك. ولقد جري الحال على تعريف الإعلان بأنه وسيلة للتبصير تسمح للعميل الافتراضي الخيار والرأي بشأن، أو الخدمة المقترحة[447]. ومن ناحية أخرى، يمكن نشر الإعلان بواسطة أية دعامة، أو من خلال المنشور الذي يوزع في الطريق العام[448].

ومن ناحية أخرى، فإن الإعلان يمكن أن يتم بطريق فرد عادي، وقد يتم عن طريق شخص محترف. ذهبت الدائرة الجنائية بمحكمة النقض لأبعد من ذلك في حكمها الصادر في 6 مايو 1998، حيث قضت بعدم أهمية أن يكون الإعلان قد تم نشره لغاية الربح، وألا ينطوي على الطابع التجاري. وبحسب موضوع ذلك الحكم، قام المتهم بتوزيع منشورات باسم جمعية الدفاع عن ضحايا الجرائم ودعي القارئ إلى تحريك دعوى

(444) Crim., 12 nov. 1997, Droit pénal, févr. 1998, p. 17

(445) Aix-en-Provence, 15 janv. 1998, Jurisdata, n° 041502 ;

(446) Crim., 12 nov. 1997, préc. ; Paris, 16 juin 1998, Jurisdata, n° 022182

(447) Agen, 15 janv. 1998, Jurisdata, n° 040689 ; crim., 6 mai 1998, n° 97-83.203, Jurisdata, n°003317

(448) A. Giudicelli, Chroniques, Rev. Sc. Crim., op.cit, P.116.

المسئولية ضد بعض النواب بالجمعية الوطنية، أو بعض المحترفين ومشاورة الجمعية في هذا الأمر، بينما كانت الجمعية خاضعة لإجراءات التصفية القضائية، ومن ثم فلم يكن في استطاعتها تقديم الخدمة المقترحة.

أخذت المحكمة بالمفهوم الواسع للإعلان من حيث دعامته والباعث عليه، وقدرت طابع الغش الذي ينطوي عليه هذا الإعلان من خلال الإحالة على معيار المستهلك المتوسط، أو على القارئ المتوسط[449]. أما عن الإعلان المبالغ فيه فإن العقاب لا يمتد إليه، بحيث أن الطابع الصاخب المستخدم في الرسالة الإعلانية يمكن أن يدفع بالقضاة إلي الحكم بعدم تحقق الجريمة.

بيد أن محكمة استئناف باريس قضت صراحة بأنه وإذا كان من المقبول تضمين الإعلان بعض صور المبالغة في الوصف، ولكن لا يجب أن تصل هذه المبالغات إلي حد التحريف الجسيم في التصوير بما يجافي الحقيقة. وعلى هذا النحو، فقد قدرت المحكمة، (" إن القيام بإجراء الإعلان من خلال الحملة الإعلانية بشأن عدم قابلية المادة المطروحة للبيع للاستخدام، يشكل جريمة إعلان كاذب طالما لم يثبت الدليل على أن هذه المادة غير قابلة للاستخدام.

في الواقع، إن المادة 121-1 من تقنين الاستهلاك تكشف بجلاء عن عناية المشرع وضع قائمة من العناصر، التي يمكن أن تحمل البيانات، أو المعطيات والعروض المضللة، أو التي يمكن أن توقع، بطبيعتها في الغلط. وبالنظر إلى هذه الخطوة التكاملية التي يخطوها المشرع، فلا يمكن القول بوجود جريمة الإعلان المضلل إلا متى كان موضوع الغش، أو التضليل أحد البيانات الواردة في القائمة القانونية[450].

وبالنظر إلي تنوع العناصر المنصوص عليها في صريح المادة 121-1، فقد تم وضع فئتين من الإعلان المضلل، على الرغم مما نجد من تداخل بين كلا الفئتين في الواقع العملي : فهناك الفئة المتعلقة بوجود، وطبيعة، وخصائص المال أو الخدمة المقترحة، أما عن الفئة الثانية، فإنها تتعلق بهوية، وجودة، وقدرات المعلن (فقد يكون المعلن صانع، أو بائع، أو مستثمر، أو ملتزم بعمل).

على أية حال، وخلال فترتنا هذه، صدر العديد من القرارات بشأن موضوع الوقائع، التي ارتبطت بأولي الفئتين المشار إليهما. تقع جنحة الإعلان الكاذب حينما يستخدم في الإعلان الخاص بعمل رحلات حول

---

(449) Axe-en-Provence, 18 mars 1998, Jurisdata, n° 040966

(450) أنظــــــــر :

G. Giudicelli-Delage, Droit pénal des affaires, 3e éd., Mémento, Dalloz, 1996, p. 154.

العالم عبارات الغرض منها إقناع العميل الافتراضي الطابع الترفيهي الراقي للطيران المقترح، بينما الخدمة المقدمة أقل من ذلك[451].

كذلك الحال، حينما يتضمن الإعلان المنشور في الصحف، والخاص بمجموعة عقارية الإشارة إلي وجود حمام سباحة، وملعب تنس بينما ومن حيث الواقع العملي لم يتم إنشاء هذه الأشغال، ولم يكن من الممكن إنشائها لعدم وجود الأرض والتمويل[452]. كما تقع هذه الجريمة ذاتها في حالة المطالبة بتبرعات خلال حملة الدعاية لصالح منظمات خيرية محددة، طالما أن هذه المنظمات لم تحصل على أية مبالغ مالية من المطلوبة للتبرع [453].

وتقع هذه الجريمة في حالة تضمين التكيت الموضوع على زجاجة النبيذ[454]، وعلى الكارتون عبارة صنع في فرنسا، بينما تم إعداد النبيذ فقط في فرنسا، ولكنه من الخارج[455]. كذلك في حالة قيام مدير شركة متخصصة في صناعة الزجاج بنشر عبارة على الزجاجة " بدون صبغات، وبدون مواد كيماوية "، بينما ثبت استخدام هذه المواد في تصنيع الزجاج الملون، والجلسرين، حيث تم العثور على هذه المواد في ورشة التصنيع[456].

بالإضافة إلي ذلك، تقع جنحة الإعلان المضلل في حالة قيام مكتب طلبات بضاعة المصحوبة بإذن تخصيص مجموعات منوه عليها بعبارة، فرصة للحصول على ساعة هدية عالية القيمة، أو قطعة مجوهرات فريدة، بما يدفع العميل إلي الاعتقاد بأن الأمر يتعلق بمزية شخصـــية. بينما ومن حيث الواقع العملي كانت الساعة الهدية متواضعة للغاية، وزهيدة القيمة، وقد تم إرسال مستندات مماثلة إلي ما لا يقل عن 250،000 شخص [457].

---

(451) Crim., 15 oct. 1997, Bull. crim., n° 337.

(452) Crim., 14 janv. 1998, n° 97-81. 690, Jurisdata, n° 001518

(453) Aix En-Provence, 4 juin 1998, Jurisdata, n° 042121

(454) A. Giudicelli, Chroniques, Rev. Sc. Crim., op.cit, P.117.

(455) Bordeaux, 10 févr. 1998, préc.

(456) Paris, 7 janv. 1998, Jurisdata, n° 020128

(457) Paris, 4 mai 1998, Jurisdata, n° 021309

والإعلان على لفافات الورد المتضمنة طباعة ملونة بعبارة أن ألوان الزهور مضمونة، بينما لم تكن الزهور تتضمن الألوان المعلنة بهذا الوصف، حيث لم يتم عمل الفحص على مجموع الأصناف التي تم بيعها[458]. كذلك الشأن في حالة تضمين صحيفة الإعلانات إعلان لبيع شقة والتنويه عن أن مساحتها 50 متر مربع بدلاً من 45 متر مربع[459].

في الواقع، وبالنظر إلي الفئة الأولي، يجدر بنا أن نشير إلي عنصر هام وهو الذي يكون في الغالب الموضوع الجوهري للإعلان المضلل: ثمن المال، أو الخدمة المقترحة. وبناءً عليه، تقع جنحة الإعلان المضلل، أو الذي يؤدي بطبيعته إلي الوقوع في الغلط، في الأمثلة التالية :

حالة مدير شركة توزيع، الذي يقترح، في إطار حملة الدعاية، مواد عالية الجودة بأثمان مغرية لفترة محددة، بينما لم يكن بعض المنتجات مهيأة خلال هذه الفترة بسبب عدم وجود بضاعة في المخازن[460]. وكذلك حالة الإعلان المسبوق بالنشرة التمهيدية عن حالة تصفية كاملة، والبيع بأثمان منخفضة لأجهزة كهربائية منزلية، بينما لا يشمل الثمن المنخفض سوى جزء صغير من هذه البضاعة.

وحالة بيع لوت من الأدوات الصحية بثمن أقل من الثمن المعروض في المحل والمنتج المباع بالثمن المعلن المشتمل على بعض القيود من حيث الكيف لم ينوه عنه في الإعلان[461]. والإعلان عن تخفيضات هامة في الروائح المعروضة للبيع بينما لم تختلف الأثمان، عن تلك التي تحددت خلال الشهرين السابقين، ولم يتم الالتزام بالقواعد المتعلقة بسعر الأساس[462].

وفي حالة الإعلان الحائطي للبيع الاستثماري لمجوهرات لصالح حاملي بطاقات التحويل، حيث تتحقق واقعة الكذب في حقيقة التخفيض المقترح حيث قام المتهم بتضخيم الأثمان العامة بصورة تتجافى والحقيقة[463]. والقيام بإصدار كوبونات رحلات حيث وبحسب الإعلان فإن هذه الكوبونات تعطي حق الإقامة بشرط أن ترسل هذه الكوبونات لشركة معينة بالاسم بغية شراء تذاكر الطيران، وبينما ومن حيث الواقع العملي،

---

(458) Paris, 5 mai 1998, Jurisdata, n° 021307

(459) Paris, 16 juin 1998, Jurisdata, n° 022182

(460) Aix-en-Provence, 15 janv. 1998, préc.

(461) Grenoble, 9 janv. 1998, Jurisdata, n° 040080

(462) Paris, 10 mars 1998, Jurisdata, n° 020745

(463) Paris, 30 avr. 1998, Jurisdata, n° 021321

يتضمن ثمن بيع التذاكر، المعلن باعتباره يتضمن إقامة مقدمة، أو مجانية لا يشمل فقط ثمن النقل الجوي، ولكن أيضا ثمن الإقامة[464].

بالنظر إلي هذه البانوراما، وعلى وجه الخصوص القرار الأخير المشار إليه، نستطيع القول بأن حكم الدائرة الجنائية بمحكمة النقض الصادر في 29 أكتوبر 1997 مثير للدهشة[465]. ففي إطار عملية استثمارية اقترحت الشركة على الجمهور، ومن خلال الإعلان الحائطي والنشرة التمهيدية موكيت وتلبيسات له مع التركيب المجاني. تم استدعاء الشركة أمام محكمة الجنح لمواجهتها بتهمة الإعلان المضلل على النحو الذي يدع الجمهور من المستهلكين يعتقد بأن التركيب كان مجاني بينما تم تمويل ثمن هذه الخدمة من خلال الزيادة في هامش الربح التجاري، وقد صدر حكم قضاة أول درجة ضد رئيس مجلس إدارة الشركة[466].

وفي سبيل إبطال هذا الحكم، فقد قضت محكمة استئناف **Douai**، من جانب لم يثبت أن كافة السلع المنتجات المعروضة للبيع بالتركيب المجاني قد طبقت معامل متنوع أعلى من المنتجات الأخرى، ولم يتم زيادة ثمنها قبل العملية الاستثمارية، ومن جانب أخر، فقد تم تعيين الخدمة المقدمة وتوريدها، ولم يتضمن الإعلان أي بيان غير صحيح، أو يؤدي بطبيعته إلى الوقوع في الغلط. وحيث أن هذا التسبيب كان كافياً، فقد كان من الواجب-بحسب محكمة الاستئناف-، فقد رفضت محكمة النقض الطعون المقدمة من النائب العام لدى محكمة الاستئناف، وكذلك المدعي بالحق المدني، وقد أكدت محكمة النقض في حكمها: (إن الإعلان عن خدمات باعتبارها مجانية بينما تم تضمين ثمنها في الثمن الخاص ببيع البضائع، وهو الموضوع الأساسي للإعلان، لا يشكل الجنحة المنصوص عليها في المادة 121-1 من تقنين الاستهلاك، طالما أن المشتري قد تم تبصيره بالثمن الشامل، الذي قام بدفعه، ولم يثبت إيقاعه في الغلط بشأن أحد العناصر الواردة في النص).

وعلى الرغم من أن الحكم الصادر في 29 أكتوبر 1997 ليس سوى حكم عادي، إلا أن العبارات التي استخدمتها الدائرة الجنائية بمحكمة النقض تنقل من الخاص إلي العام، ولكن على نحو غير ملائم. فنحن نشك في ملائمة الصياغة التي تمت بطريق محكمة النقض، وذلك بالنظر إلي نص القانون والغايات التي يسعى إلى إدراكها.

---

(464) **Aix-en-Provence, 25 mars 1998, Jurisdata, n° 041494**

(465) **Bull. crim., n° 362 ; JCP 1998.11.10138, obs. Critiques J. Casey**

(466) **A. Giudicelli, Chroniques, Rev. Sc. Crim., op.cit, P.116.**

وبرغم ما جاء في حكم محكمة النقض، إلا أننا نتساءل عما إذا كان من الممكن القول بأن الخدمة كانت مجانية، بينما تم تضمين ثمنها في ثمن البيع؟، ألا يخاطر المستهلك المتوسط في الاعتقاد، بطريق الخطأ بأن المعلن يتحمل ثمن الخدمة، بينما هو الذي يدفعه في النهاية ؟

نحن ندرك بأنه ومتى كان الثمن موضوع العملية الاستثمارية لم يتم بعد زيادته ففي هذه الحالة يعن لنا أن نتساءل عما إذا كانت الخدمة المقدمة في حالة الشراء قد قدمت بالفعل من عدمه. بيد أننا لا نشايع من جانبنا هذا الحل، الذي يدفع إلى الاعتقاد- في عبارات على قدر كبير من التعميم-، وفي مثل هذه الحالة للمستهلك المبصر بالثمن المدفوع، أن الإعلان لم يؤدي إلي الوقوع في الغلط بشأن أحد العناصر الواردة في صريح نص القانون، بينما يحرم نص القانون العروض التي تؤدي إلى الوقوع في الغلط حينما تنصب على ثمن وشروط بيع الأموال، أو الخدمات، موضوع الإعلان[467].

إن الفئة الأخرى للإعلان المضلل، وهي تلك التي تتعلق بهوية، وجودة، وقدرات المعلن. هنا يمكننا الرجوع إلي العديد من الأحكام القضائية التي صدرت بشأن هذه الفئة من الإعلان المضلل على وجه الخصوص. وعلى هذا النحو، يتحقق وصف جنحة الإعلان المضلل المنصوص عليها في المادة 121-1 من تقنين الاستهلاك على الحالات الآتية:

حالة المعلن الذي يقدم خدمة عقارية على النحو الذي يدعو إلى الاعتقاد بأنه موكل من عملاء أجانب للقيام بشراء عقارات، بينما ومن حيث الواقع العملي ينحصر دوره في مجرد إرسال الملفات إلي الوكالات العقارية الأجنبية[468]. كذلك الحال، حينما يستخدم موزع الخمور صفة المالك الحاصد للكروم بينما وفي المجال الزراعي، نجد أن لفظ المالك يعني الملكية العقارية ولفظ الحاصد، هو الشخص الذي يقوم بالزرع والحصاد لثمرة إنتاجه[469].

كذلك في حالة قيام مدير شركة تبديل المنزل بالإعلان في الصفحات الصفراء بحولية فرانس تيليكوم، حيث نوه في الإعلان عن أن شركته استفادت من العلامة "**NF Service**"، بينما ومن حيث الواقع العملي لم يكن يملك شهادة مطابقة[470].

---

(467) A. Giudicelli, Chroniques, Rev. Sc. Crim., op.cit, P.118.

(468) Agen, 8 juill. 1998, Jurisdata, n° 043571.

(469) Bordeaux, 15 janv. 1998, préc.

(470) Susan W. Brenner, Law in an Era of “Smart” Technology, ibid, P 87.

على ذات المنوال، نشير إلي حالة مدير مدرسة الفنون بنشر إعلان في صحيفة الإعلانات يبين فيه أن المدرسة تصدر دبلومات معتمدة من الدولة، بينما لم تحصل المدرسة على هذا الاعتماد من الدولة في الواقع العملي[471]. والتنويه في البريد الذي يقترح تقديم مساعدة للمحترفين في حالة التعثر المالي، على أنه صادر عن المفوضية العليا للشركات المتعثرة، بينما تخصص وظيفة المفوضية العليا للأعضاء النيابة العامة، وهو ما يمكن أن يوجد حالة من الخلط مع المنظمة العامة .[472]

كذلك يتحقق وصف الإعلان المضلل في حالة كتيب الاستقبال الخاص بدار المسنين، متى تضمن الإعلان بيان بأن الدار بها تجهيزات طبية وصيدلية بخلاف الواقع، حيث تتم العناية الطبية من خلال ممارسين خارجيين[473].

صفوة القول، في مجال الإعلان المضلل، وعلى غرار الحال بالنسبة للمجالات الأخرى، يجوز إعفاء مدير الشركة من المسئولية ـ متى برهن على أنه فوض سلطاته لتابعه. وهناك العديد من القرارات التي تؤكد أن صحة التفويض رهن بأن يتم للشخص الذي يملك الاختصاص، والسلطة، والوسائل الضرورية[474]، والتفويض يكون مقبولاً في ذات الشروط.

بالإضافة إلي ذلك، فقد أيدت الدائرة الجنائية بمحكمة النقض حكم محكمة استئناف **Aix-en-Provence**، حيث قضت بأن المستند المعنون بتفويض سلطات والذي قدم لأول مرة أمام محكمة الاستئناف، ولم يتضمن وصف المفوض إليه، ولكن فقط مجرد توقيع مختلف عن التوقيع الموضوع على محضره الرسمي المحرر بالاستماع لدى البوليس، لا يعفي المدير العام للشركة من المسئولية الجنائية عن الإعلان المضلل، الذي جرى استخدامه.

رابعا : موضوع الإعلان في القانون المصري: بالنظر إلي قانون حماية المستهلك رقم "181" لسنة 2018 ولائحته التنفيذية، يتضح أن الضوابط القانونية والالتزامات التي وضعها المشرع على عاتق المورد والمُعلن كل

---

[471] **Paris, 27 janv. 1998, Jurisdata, n° 020169.**

[472] **Paris, 25 févr. 1998, préc.&**

[473] **Paris, 3 juin 1998, Jurisdata, n° 021960**

[474] **Aix-en-Provence, 15 janv. 1998, préc.**

الالتزامات التي من شأنها أن تؤدي إلى وصول السلعة إلى المستهلك دون أي مخاطر[475]. بينما كانت اللائحة التنفيذية محددة لصور الإعلان الخادع والذي قد يؤدي إلى وقوع المستهلك في لغط أو غلط نعرض لها في المبحث التالي.

ومما تقدم، يتبين أن الإعلان كوسيلة لعرض السلع والخدمات علي المستهلك عبر شبكة الإنترنت، يشكل بشتى صوره وأشكاله وأساليبه أخطارا هامة، تستوجب حماية المستهلك في هذه المرحلة من التعامل الاقتصادي، إلا أن المشرع المصري تشابه مع موقف المشرع اللبناني في التوسع في النص على أيا كانت وسيلة نشر الإعلان، ولم يشابه موقف المشرع الفرنسي في إقرار نصوص عقابية مستقلة توضح جرائم الإعلان الخادع عبر شبكة الإنترنت وهذا ما سوف نتطرق له لاحقا في بحثنا.

المبحث الثاني: وسائل حماية المستهلك في مواجهة الإعلانات الإلكترونية الكاذبة

يكون الإعلان الإلكتروني المضلل جريمة إذا توافر فيه عنصرين الأول مادي والذي يتكون من وسيلة دعائية، وهي عبارة عن شبكة الإنترنت، أو بعض الوسائط الإلكترونية الأخرى كالهواتف المحمولة والتلفزيون حيث يمكن أن تستخدم هذا الوسائل بطريقة احتيالية تضلل المستهلك وتوقعه في الخطأ[476] الذي يبنى عليه عقيدته في شراء السلع والخدمات المعروضة عبر الإنترنت، كذلك يجب أن يتضمن العنصر الأول وجود معلومات مضللة أو كاذبة من شأنها إيقاع المستهلك في الغلط، وأن تكون المعلومات المضللة التي توقع في الغلط أحد العناصر الأساسية المكونة للسلعة أو الخدمة.

أما العنصر الثاني من عناصر جريمة الإعلان التجاري الإلكتروني المضلل فهو القصد الجنائي الذي هو أساس قيام المسؤولية الجنائية، لذلك سوف نتعرض إلي قواعد حماية المستهلك في مواجهة الإعلانات الإلكترونية في **المطلب الأول**، والمسؤولية الجنائية عن الإعلانات الخادعة في **المطلب الثاني**.

---

(475) أنظر المواد من 3 إلى 7 من نصوص قانون حماية المستهلك المصري رقم 181 لسنة 2018. كما انظر المواد رقم 2 الى 8 من اللائحة التنفيذية لذات القانون، وقد تناول بعض الفقهاء حماية المستهلك في مرحلة التفاوض، فهناك التزامات متبادلة تقع على عاتق الأطراف في التفاوض ومن هذه الالتزامات: الالتزام بمبدأ حسن النية، والالتزام بالإعلام والالتزام بالتعاون، والالتزام بعدم إفشاء المعلومات السرية، وهنا يلاحظ عدم التكافؤ ما بين الطرفين" المزود والمستهلك". انظر في ذلك د/أسامة أحمد بدر، حماية المستهلك في التعاقد الإلكتروني، مرجع سابق. ص 181،180.

(476) د/أحمد إبراهيم عطية، النظام القانوني للإعلان في القانون المدني، الطبعة الأولى، دار النهضة العربية، 2006، ص 384.

المطلب الأول: قواعد حماية المستهلك في مواجهة الإعلانات الإلكترونية

تقوم حماية المستهلك في مواجهة الإعلانات الإلكترونية المضللة على قاعدتين أساسيتين، الأولى تتعلق باشتراط وضوح الإعلان الإلكتروني الفرع الأول، أما الثانية، فتتحدث عن منع الإعلان الإلكتروني المضلل الفرع الثاني .

الفرع الأول: اشتراط وضوح الإعلان الإلكتروني

يجب أن يكون الإعلان الإلكتروني[477] واضحا وهذا يعني أن يتضمن الإعلان البيانات الكافية عن السلعة أو الخدمة المقدمة وهذا ما أوضحته في موقف التشريع الفرنسي سابقاً، فوضوح الإعلان الإلكتروني من شأنه أن يخلق لدى المستهلك تفكير واعي وأن يبصره بالسلعة أو الخدمة المعروضة عليه، مما يكون لدية إرادة واعية مستنيرة لدي وهو بصدد الإقبال علي شراء السلعة أو الخدمة[478].

فالإعلان الإلكتروني يجب أن يكون متميزا بوضوحه ولا يوجد به غموض[479]، بحيث يتم تزويد المستهلك بمعلومات كافية وواضحة عن السلعة أو الخدمة المعروضة بما يسمح للمستهلك الموافقة أو رفض قيام التعاقد بناء على وعى وإدراك كاملين[480].

الأمر أن التشريع المصري، في قانون حماية المستهلك رقم "181" لسنة 2018 قضت المادة "4" منه بأنه على كل مورد ومعلن إمداد المستهلك بالمعلومات الصحيحة عن طبيعة المنتج وخصائصه وتجنب ما قد يؤدى إلى خلق انطباع غير حقيقي أو مضلل لدى المستهلك أو وقوعه فى خلط أو غلط. ويعفى المعلن من المسؤولية متى كانت المعلومات التي تضمنها الإعلان فنية يتعذر على المعلن المعتاد التأكد من صحتها، وكان المورد قد أمده بها، كما يجب أن تكون تلك المعلومات والبيانات باللغة العربية.

ويلاحظ من النصوص السابقة أن المشرع المصري اهتم بحماية المستهلك من خلال إلزام المزود بإعلامه وتبصيره بمعلومات واضحة عن المنتج أو الخدمة المعروضة، بحيث لا يكون هناك خداع أو تغرير، كما ألزم المشرع أيضا المزود بأن يمتنع عن الإعلان أو التسويق للمنتجات والخدمات التي تلحق ضررا بحقوق المستهلك، وهذا ما أخذ به المشرع الفرنسي في المادة 121 من قانون الاستهلاك.

---

[477] أنظر المادة 3 من اللائحة التنفيذية لقانون حماية المستهلك المصري رقم 181 لسنة 2018.

[478] د/ ممدوح خالد إبراهيم، حماية المستهلك في المعاملات الإلكترونية، مرجع سابق، ص. 89. كما انظر لذات المؤلف، أمن الجريمة الإلكترونية، الدار الجامعية، 2010، ص 126.

[479] د/ محمد أحمد أبو سيد أحمد، حماية المستهلك في الفقه الإسلامي، الطبعة 1، لبنان، دار الكتب العلمية، 2004، ص 286.

[480] تلعب الإعلانات الإلكترونية دورا بالغ الأهمية في التجارة الإلكترونية، حيث ازدادت نفقات الإعلان الإلكتروني في الولايات المتحدة بشكل طردي في الأعوام الأخيرة.

الفرع الثاني: منع الإعلان الإلكتروني المضلل

يعتبر الإعلان التجاري مظهر من مظاهر المنافسة المشروعة، وعامل من عوامل التسويق وأداة من أدوات إعلام الجمهور بالمنتجات والخدمات. وكما علمنا سابقا بأن الإعلان المضلل هو " الإعلان الذي يكون من شأنه خداع المستهلك، أو يمكن أن يؤدي إلي ذلك "[481]، كما عرف أيضا بأنه " الإعلان المتضمن معلومات تهدف إلي الوقوع في خلط وخداع فيما يتعلق بعناصر وأوصاف جوهرية للمنتج .[482]

فالإعلان التجاري المضلل هو الذي يؤدي إلى خداع المستهلك من خلال تضمنه معلومات مغلوطة بعناصر وأوصاف جوهرية خاطئة في السلعة أو الخدمة المعروضة، وبالتالي يجب أن تكون له ضوابط تحكم مشروعيته، من خلال مشروعية محل الاعلان، والبيانات التي يجب أن يتضمنها الإعلان، وأن يكون موافق الضوابط الشكلية للإعلان الإلكتروني، كما يجب أن تكون هناك رقابة سابقة ولاحقة على نشر الاعلانات[483].

هذا وتحدث توجيه المجلس الأوروبي الصادر في 15 سبتمبر 1984 بالمادة الثانية منه عن الإعلان المضلل أو الخادع بأنه أي إعلان بأي طريقة كانت، يحتوي في طريقة تقديمه علي أي تضليل لهؤلاء الذين يوجه إليهم الإعلان، كما نصت المادة الثالثة من التوجيه الأوروبي السابق علي أن الإعلان المضلل يقـع عـن طريـق إغفال إحدى الخصائص الجوهرية للسلعة المعلن عنها .[484]

كما تناول قانون حماية المستهلــك المصري واللائحة التنفيذيــة للقانون في بعض مواده ضرورة وضــوح الإعلان، وأن تكون المعلومات غير مغلوطة[485]، وعاقــب علي الادعاء أو الإيهام بأن السلعة تتمتع بشهادة الجودة، أو إخفاء أية مادة أو سلعة مخزونة لدى المنتج عن أي شخص يريد شراءها دون سبــب مشروع.

---

[481] د/ أبو العلا علي النمر، المشكلات العملية والقانونية في التجارة الإلكترونية، دار النهضة العربية، 2004، ص209؛ د/ ممدوح خالد إبراهيم: حماية المستهلك في المعاملات الإلكترونية، مرجع سابق، ص 92. كما انظر لذات المؤلف، أمن الجريمة الإلكترونية،مرجع سابق، ص 129.

[482] د/ سميحة القليوبي، غش الأغذية وحماية المستهلك، مؤتمر حماية المستهلك في القانون والشريعة، جامعة عين شمس،1995. ص 135.

[483] د/ هدى حامد قشقوش، الإعلانات غير المشروعة، مرجع سابق، ص43 وما بعدها.

[484] د/إبراهيم ممدوح خالد، حماية المستهلك في المعاملات الإلكترونية، مرجع سابق، ص 91.

[485] انظر نصوص كل من المادة 9 من قانون حماية المستهلك المصري رقم 181 لسنة 2018، أنظر أيضا المادة 8 من اللائحة التنفيذية لذات القانون بشأن كيفية تحديد الإعلان الخادع.

وبالتالي فإننا نرى بضرورة حماية المستهلك الالكتروني من الوقوع في الخطأ ، فقد أوجبت المادة الرابعة والخامسة من ذلك القانون على: " كل مورد ومعلن إمداد المستهلك بالمعلومات الصحيحة عن طبيـــعة المنتج وخصائصه، وتجنب ما قد يؤدي إلي خلق انطباع غير حقيقي أو مضلل لدى المستهلك، أو وقوعه في خلط أو غلط"، ويستفـــاد من هذا النص أن المشرع المصري أوجد التزاما على المعلن والمورد بإعلام المستهلك بالمعلومات الصحيحة عـــن طبيعة السلعة، وخصائصها بما يحمي المستهلك من تكوين اعتقاد غيـر صحيـح أو مضلل، كمــا وضــع المشرع المصري عقوبة جنائية[486]، علي المعلن في حالة قيامه بتضليل المستهلك، أو ارتكاب أفعال تؤدي إلي الوقوع في خلط أو غلط.

إلى جانب ذلك فإننا نرى أنه عندما يكون الإعلان التجاري واضحا فإن ذلك يؤثر إيجابيا على المستهلك الإلكتروني، حيث أنه يكون على بينة من كل ما يتعلق به السلعة أو الخدمة المرغوبة، ليس هذا فقط وإنما يكون المُعلن في مأمن من أي إدعاء من جانب المستهلك بعد ذلك تتعلق بهذا الأمر، كما أن المُعلن يتجنب بذلك ما قد يؤدي إلي خلق انطباع غير حقيقي أو مضلل لدى المستهلك بعد إتمام التعاقد.

الفرع الثالث: ضرورة أن يكون الإعلان باللغة العربية او مترجم الى اللغة العربية

لم يدخر المشرع الفرنسي جهداً في حماية المستهلك وحماية اللغة الفرنسية، فلقد قام بإصدار قانون 31 ديسمبر 1975 الذي جعل استخدام اللغة الفرنسية في الإعلانات المكتوبة والشفوية عن المنتجات والخدمات أمر إلزامياً، إلا أن هذا القانون السابق ذكره لم يكن شاملاً للإحاطة بكافة أنواع الحماية للمستهلك من الإعلان والإعلانات إذا أصدر القانون رقم 4 أغسطس 1994 والذي عُرف باسم قانون Loi Toublon والذي عالج الموضوع من جديد بعد إلغاء القانون رقم 31 ديسمبر 1975.

وتناول القانون الجديد مسألة استخدام اللغة الفرنسية في الإعلانات وأكد علي ضرورة الإلتزام بها[487] في كافة الإعلانات التي تخاطب جمهور المستهلكين وهو ما فرضته المادة 1/2 من القانون من استخدام اللغة الفرنسية في تسمية وعرض طريقة استخدام الأموال والخدمات وشروط ضمانها في تحديد القوانين وإيصالات المخالصات.

---

[486] **انظر نص المادة 64 من قانون حماية المستهلك المصري رقم 181 لسنة 2018.**

[487] **Ch. Gavalda, et Plaskowski (N.), Droit de l'audiovisuel, cinéma, Télévision, vidéo, multimédia, 3ème éd., Lamy,. 3ème éd., S. 1995, n° 837, P.715.**

كما نصت المادة 3/2 من القانون على أن تطبق نفس الأحكام على كل الإعلانات المكتوبة والمنطوقة والمرئية والمسموعة. ومن ذات القانون أيضاً نصت المادة الثالثة علي إلزام استخدام اللغة الفرنسية في كل الإعلانات التي تتم في الطرق العامة أو في الأماكن المفتوحة للجمهور أو في وسائل النقل الجماعي وتكون مخصصة لإعلام الجمهور ولم يستثنى من أحكام القانون إلا أسماء المنتجات المسماة بأسماء أجنبية.

وعلى ذلك قضت محكمة النقض الفرنسية بمخالفة الإعلان للقانون عندما استخدم اللغة الانجليزية ولم يصحبها بترجمة باللغة الفرنسية، كما قضى استخدام الإعلان أسماء مستوحاة من اللغة الانجليزية بالمخالفة لأحكام القانون الذي يفرض على المعلنين استخدام اللغة الفرنسية[488] فالقانون الفرنسي لم يحظر كما سبق وأن ذكر بصفة مطلقة الإعلانات باللغة الأجنبية، وإنما تطلب في حالة استخدامها بضرورة مصاحبته بترجمة باللغة الفرنسية على أن تكون واضحة مسموعة أو مقروءة أكثر من اللغة الأجنبية.[489]

وبالنسبة لمصر فقد نصت المادة 64 عقوبات من القانون 181 لسنة 2018 كالاتى" يعاقب بغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسمائة ألف جنيه أو مثل قيمة المنتج محل المخالفة أيهما أكبر، نل مورد خالف أحكام أي من المواد : (3، 4، 5، 6، 7، 12، 14، 16، 18، 21، 35، 38، 40/ فقرة أولى وثانية، 55، 56/ فقرة أولى، 62/ فقرة أخيرة) من هذا القانون.

ويعاقب بذات العقوبة كل من خالف القرارات الصادرة نفاذًا لحكم المادة (33/ فقرة أولى) من هذا القانون، وللمحكمة أن تحكم بغلق مركز الخدمة والصيانة المخالف لمدة لا تجاوز ستة أشهر.

وإذا نظرنا أيضاً في بعض المنتجات خاصة المنتجات الإلكترونية ذات التقنية العالية، وجدنا الكتالوج الخاص بشرح كيفية استخدامها يتكون من عديد من اللغات إلا اللغة العربية، رغم أنها تشتمل علي لغات أكثر انتشاراً وأقل تحدثاً على المستوى الرقعة الجغرافية ورغم ذلك نجدها من ضمن اللغات التي تشرح كيفية استخدام وتشغيل المنتج.

ويعاب على المسئولين عن منافذ دخول هذه المنتجات وعلي مستورد السلعة، وأخيراً والأكثر مساءلة هو جهاز حماية المستهلك الذي لم يتدخل لحل هذه المشكلة وهي إما بالمنع من تداول هذه السلعة أو إلزام المنتج

---

[488] **Cass. Crim 25 Avril 1989, P. 472. Responsible sur . see.**

www.courtcassation.com

[489] **د/ سيد محمد سيد شعراوي، الحماية المدنية للمستهلك في عقود البيع الإلكتروني، مرجع سابق، ص 105.**

بإعادة ترجمة الكتالوج إلي اللغة العربية علي حسابه، ويأتي هذا لأن المنتج والمستورد لا يجد من يحاسبه أو يوجهه إليه مسئولية مخالفة ذلك والعقاب عليها.

وهناك من القرارات والقوانين تعالج هذه المسألة بصورة جزئية، ومن ثم فإنها غير فعالة في بعض الأحيان فهناك قرارات استلزمت أن يكون هناك إعلام عن السلعة أو الخدمة باللغة العربية، كما هو الشأن في قرارات وزير الصناعة والثروة المعدنية رقم 58 لسنة 1980 الذي ينص في مادته الأولي علي أن " تلتزم المنشآت الصناعية المحلية المنتجة للمواد الغذائية بأن تضع على عبواتها الغذائية بطاقة تشمل البيانات التالية ..." ومنها:

1- يجب أن تكتب البيانات باللغة العربية وبخط واضح غير قابل للمحو، ويجوز كتابتها بلغة أخرى أو أكثر إلي جانب ذلك.

2- قرار وزير الصناعة رقم 266 لسنة 1981 الذي ينص في مادته الثانية على أنه يجب أن تكتب هذه البيانات باللغة العربية بخط واضح غير قابل للمحو وتكتب أما مباشرة علي العبوة أو علي بطاقة تثبت علي العبوة، ويجوز أن تكتب هذه البيانات بلغة أجنبية أخرى أو أكثر إلي جانب اللغة العربية.

وفي نفس السياق صدرت قرارات أخرى مثل قرار وزير الاقتصاد رقم 263 لسنة 1981 بالرقابة علي المستورد من المنظفات الصناعية المنزلية غير السائلة.

فهذه القرارات متعددة المصادر، فبعضها صادر عن وزير التجارة[490]، وبعضها صادر من وزير التموين[491]، وبعضها صادر عن وزير الصحة[492]، والبعض الآخر صادر عن وزير الصناعة والثروة المعدنية[493].

وهذا النوع في القرارات يؤدي إلي صعوبة تحديد من لهم صفة مأموري الضبط القضائي فيما يتعلق بتطبيق هذه القرارات هذا بالطبع يؤدي أيضاً إلي صعوبة الوقوف على الجزاءات المقررة. بالإضافة إلي أن هذه الجزاءات تختلف من قرار لآخر.

---

(490) قرار رقم 225 لسنة 1978 الرقابة على المستورد من الألبان المجففة والقرار رقم 26 لسنة 1978 الخاص بالرقابة على المستورد من الجبن.

(491) القرار رقم 252 لسنة 1961 في شأن تنظيم وتعبئة وتجارة الشاي والبن.

(492) القرار رقم 381 لسنة 1982 بشأن المواد الغذائية المسموح بإضافة مواد ملونة إليها والمعدل بالقرار رقم 136 لسنة 1983 والقرار الوزاري 389 لسنة 1984 و17 لسنة 1985.

(493) القرار رقم 58 لسنة 1980 الصادر في 1980/11/24.

ولا شك أن هذه السياسة التشريعية سياسة معيبة، فلا يتصور أن تظل السلعة متداولة ولا يصدر القرار إلا بعد تواجد السلع والخدمات بالسوق وبها مخالفة قانونية وتبدأ حين ذلك المعالجة.

فليس هناك رؤية لمبدأ الوقاية خيراً من العلاج، كما أنه من الصعب أن يصدر قرار وزاري بقدر عدد السلع والخدمات المتداولة.

ولا يختلف أمر القوانين كثيراً عن القرارات الوزارية، فهي أيضاً ليست حاسمة في هذا الشأن فبعضها ينصب علي سلعة معينة دون غيرها، كما هو الشأن بالنسبة للقانون رقم 10 لسنة 1966 بشأن مراقبة الأغذية وتنظيم تداولها المعدل بالقانون رقم 30 لسنة 1976 والقانون رقم 106 لسنة 1980، والقانون رقم 1 لسنة 1994 بشأن الوزن والقياس والكيل والقانون رقم 68 لسنة 1976 بشأن المراقبة على المعادن الثمينة المعدل بالقانون رقم 3 لسنة 1994.

أما القوانين ذات الطابع العام فإنها تتمثل في القانون رقم 48 لسنة 1941 الخاص بقمع الغش والتدليس والثاني قانون رقم 57 لسنة 1939 الخاص بالبيانات والعلامات التجارية المعدل بالقانون رقم 143 لسنة 1949، 513 لسنة 1953، 569 لسنة 1954، ورقم 205 لسنة 1956، و 65 لسنة 1959.[494]

والثابت هو القانون رقم 115 لسنة 1958 الخاص باستعمال اللغة العربية، وأخيراً فإن المنتج لأي سلعة سواء كانت محلية الصنع أم مستوردة من الخارج ويكون مسئولا عما تحدثه هذه السلعة من أضرار، طالما أنها لا تحمل تحذيراً واضحاً من مخاطر باللغة العربية، ولا يغني عن ذلك أن يكون هذا التحذير مكتوباً بكل لغات العالم الأخرى، لأن التحذير بلغة أجنبية يعد تحذيراً غير واضح وغير مفهوم[495].

المطلب الثاني: الجوانب التطبيقية لجريمة الإعلان المضلل

لعل الإعلانات التي يتخذ المعلن الإنترنت كوسيلة للترويج عن السلع والخدمات التي يحترف التجارة بها، وللتوسع التكنولوجي الملحوظ فإن جرائم الإعلان الإلكتروني تتخذ صور كثيرة والمسؤولية الجنائية عنها أيضا تستوجب تحديد دقيقا لكي نواجهه تلك الجرائم.

---

[494] د/ ياسر أحمد كامل الصيرفي، حماية المستهلك وضرورة الإعلام عن السلع والخدمات باللغة القومية، مجلة البحوث القانونية والاقتصادية- كلية الحقوق، جامعة المنصورة، العدد 43 طبعة 2008، ص 27.

[495] د/ ياسر أحمد كامل الصيرفي، حماية المستهلك وضرورة الإعلام عن السلع والخدمات باللغة القومية، مرجع سابق، ص 38.

وقبل الخوض في الحديث عن الأساس القانوني لقيام المسؤولية الجنائية، لا بد من التساؤل أولا عن المسؤول جنائيا عن الإعلان الخادع، وتجنبا لأي تفسير أو اجتهاد فقد اعتبر القانون أن المعلن الذي يباشر الإعلان لحسابه الخاص مسئول بصفة أصلية عن المخالفة، بمعنى أن صاحب البضاعة الذي أنجز الإعلان لحسابه هو المسئول الأصلي عن المخالفة، أما القائمون بالإعلان كانوا شخصا ذاتيا أو شركة يسألون كمساهمين أو مشاركين بحسب الظروف وفى هذه النقطة قد أوضحنا سابقا موقف المشرع الفرنسي من مسئولية من بث الإعلان ومعاقبته بنفس عقوبة الفاعل الأصلي.

وبالنظر إلى خطورة تلك الإعلانات وما قد تحتويه من خداع قد يؤدي إلى الإضرار بالمستهلك سواء في صحته أو حياته أو ماله فقد كان من اللازم البحث عن الأساس القانوني لقيام المسؤولية الجنائية للخادع حتى تكون المعاملات التجارية و سلامة المستهلك في مأمن. وفي هذا الصدد يمكن الاستناد إلى إمكانيتين:

أولا- إمكانية الاستناد إلى جريمة النصب: إن جريمة النصب تقوم على أساس الاستيلاء على أموال المجني عليه (المستهلك في موضوعنا) برضاه وذلك باستعمال الحيلة و الخداع و المكر. كما أكدت ذلك المادة 336 من قانون العقوبات المصري، هذه الجريمة التي تفرض عرض ركنيها المادي و المعنوي.

1:الركن المادي : و يتمثل في استعمال الاحتيال، و المساس بمصالح المجني عليه، بخصوص استعمال الاحتيال فإنه يتم بتأكيدات خادعة، و إخفاء وقائع صحيحة، أو باستغلال ماكر لخطأ وقع فيه الغير. و تحتوي التأكيدات الخادعة على كل وسائل الكذب المؤيدة بوقائع خارجية من شأنها خداع المستهلك و تضليله في الإعلان المقدم له. أما مجرد الكذب فلا يكفي لوحده لقيام جريمة النصب لأن أقصى ما يشكله هو التدليس المدني الذي لا يقع تحت تأثير الحماية الجنائية.

ويتحقق ذلك بذكر أمر مخالف للحقيقة سواء كان هذا الأمر مختلفا برمته أو كان مُحرفا في بعض جوانبه من خلال الوسائل السمعية و البصرية أو ما هو مكتوب فقط فالإعلان عن السلعة في الصحافة إذا كان مضللا عد نصباً إذا تم تدعيمه بمظاهر خارجية مؤثرة على المستهلك كاستخدام المستخدمين لدى الصحافة.

أما فيما يتعلق بالاستغلال الماكر لخطأ وقع فيه الغير، فالمقصود به وقوع المستهلك من تلقاء نفسه أو بفعل شخص آخر.أي توهمه للواقع على غير حقيقته و مثاله أن يعتقد المستهلك غلطا أن الفاعل (القائم بالإعلان) مازال ممثلا للشركة التي يتعامل معها فيعمد الجاني الذي انتهت مهمته كممثل للشركة المُعلنة و التي يشهد لها بالجودة إلى إيهام الضحية و إضلاله، بمنتجات خادعة بغية الاستيلاء على ماله.

وبخصوص المساس بمصالح الضحية، فإن جريمة النصب تتم بالاستيلاء على ماله بعد تسليمه. لكن هذا لا يؤثر على قيام هذه الجريمة حتى و لو لم يقع الاستيلاء متى أتى الجاني تصرفا يمس بمصالحه أو مصالح غيره نتيجة نشاط المحتال، ومثاله الإعلان الخادع الذي يود المعلن من خلاله أن يوقع المستهلك في شباك النصب و تم اكتشافه. وهذا ما يستفاد من المادة 336 من القانون الجنائي التي تجعل من النصب جريمة شكلية يكتفي فيها بإتيان الفعل.

2: الركن المعنوي: في جريمة النصب يتطلب لقيامه توفر القصد الجنائي الخاص[496] بحيث أن هذه الجريمة تصنف ضمن الجرائم العمدية أي أن تكون للجاني في إعلانه الخادع النية الإجرامية في الإضرار بمصالح الضحية، عن طريق وسائله الاحتيالية بهدف تحقيق فائدة مالية. كان المشرع واضحا لما استعمل العبارة التالية (بقصد الحصول على منفعة مالية له أو لشخص آخر) أما إذا استعمل الجاني هذه الوسائل الاحتيالية نتيجة غلط أو جهل فان القصد الجنائي ينتفي هنا، وبالتالي لا وجود لجريمة النصب. ويرجع الأمر في تقديره للقاضي الذي يقضي من خلال الوقائع المعروضة أمامه مدى توفر هذا القصد من عدمه، و له أن يستعين في ذلك بكل وسائل الإثبات القانونية مع إلزامه بتبيان تلك الوقائع في الحكم لأن ذلك يدخل في التعليل الواجب للأحكام. إضافة إلى جريمة النصب يمكن الاستناد أيضا إلى جريمة الغش.

ثانيا: مدى إمكانية الاستناد إلى جريمة الغش: إذا كان الخداع والمغالطة المكون لجريمة النصب المنصوص عليها في المادة 336 من القانون العقوبات يتم بواسطة تأكيدات خادعة أو كتمان وقائع صحيحة، فإن الإعلانات الخادعة المكونة لجريمة الغش يتم بأفعال تقع على البضاعة نفسها ليقع المشتري في الغلط المطلوب و يتوهم بأن بضاعة ما هي من جنس أو طبيعة بضاعة أخرى هي المطلوبة، وبالتالي فالغش بهذا المعنى يؤدي إلى التداخل بين أفعال خداع المستهلك و بين أفعال غش في البضاعة ذاتها[497].

و بالاستناد إلى قانون قمع الغش والتدليس رقم "48"لسنة 1941 المعدل بالقانون رقم "281" لسنة 1994 يتبين أن هذا القانون ينص على مجموعة من الجرائم اعتبرتها جرائم غش غير أنه لاعتبارها كذلك لا بد من التطرق إلى ركنيها المادي و المعنوي أيضا[498].

---

[496] راجع في ذات المعنى: د/ محمود نجيب حسني، النظرية العامة للقصد الجنائي، دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، دار النهضة العربية، القاهرة، 1988،ص 131.

[497] الطعن رقم 539 لسنة 13 ق، جلسة 1943/2/15، مكتب فني، سنه 6، قاعدة رقم 112، ص 162.

[498] المستشار/ معوض عبد التواب، الوسيط في شرح جرائم الغش والتدليس وتقليد العلامات التجارية، دار المطبوعات الجامعية، الطبعة الرابعة، 1998، ص17.

بشأن الركن المادي لجريمة الغش[499]، وبالنظر إلى المادتين الأولى و الثانية من القانون المذكور يعد مرتكبا الغش عن طريق الخداع أو التزييف كل من غالط المتعاقد بوسيلة ما، وذلك عن طريق إنجاز الفعل الممنوع قانونا بشكل تتحقق معه عناصره سواء بتزييف البضاعة أو عدم وصف حقيقتها أو كميتها أو عددها ، ويتحقق بإضافة مادة غريبة إلى السلعة أو بانتزاع شيء من عناصرها النافعة أو بإخفاء البضاعة تحت مظهر خادع من شأنه غش المشتري أو بالغلط أو بإضافة مادة مغايرة لطبيعة البضاعة و إظهارها في صورة أجود مما هي عليه في الحقيقة. وبالتالي وضعها محل إعلان تجاري معروض للتسويق من طرف المستهلك[500]. على أن يترتب عن الفعل الصادر من الجاني نتيجة إجرامية، و إلى جانب ذلك يجب أن تتحقق العلاقة السببية بين الفعل و النتيجة و هي الرابطة التي تسمح بإسناد النتيجة إلى سلوك إجرامي معين فتقوم بذلك المسؤولية الجنائية للجاني (والتي تخضع للسلطة التقديرية للقاضي الجنائي الذي يبقى ملزما ببيان الوقائع التي اعتمد عليها للقول بوجود تلك العلاقة أو عدم وجودها، وبالتالي تحقق الجريمة.

ولعل ما يستوقفنا هنا قبل الدخول في الركن المعنوي لهذه الجريمة هو أن المشرع المصري قد أغفل النص عن الإعلان عن السلع المغشوشة في قانون قمع الغش والتدليس، ولكنه نص عليها في موضع آخر بعد ذلك مدة طويلة، ولكن هذا على عكس المشرع الفرنسي الذي كان واضحا في البداية وجرم الإعلان الكاذب بقانون 27 ديسمبر 1973، والذي أعيد صياغته بعد ذلك في المادة 121 سالفة الذكر من مدونة الاستهلاك الفرنسية الصادرة في 26 يوليو 1993، رغم أن جريمة الإعلان الكاذب جريمة عمدية، والدافع وراء ذكر ذلك هو أن موقف المشرع الفرنسي دائما استباقي في النظر واستقرار الواقع ومواجهة المشكلات حتى وإن لم تقع ، وهذا ما نرجوه من المشرع المصري في أن يحذو حذوه.

أما فيما يتعلق بالركن المعنوي لجريمة الغش، فتقوم جرائم الغش على القصد الجنائي أي أنها جرائم عمدية حيث يتوافر القصد الجنائي في جريمة الغش بمجرد علم الجاني بأن الوسيلة التي يتبعها من شأنها أن تؤدي إلى خداع المستهلك، وأنه يريد من ورائها الوصول إلى تلك النتيجة في إحدى صورها الأربعة و التي تكون محل الإعلانات التجارية الخادعة. توافر القصد الجنائي يخضع في تقديره إلى سلطة قاضي الموضوع و الذي يقدم بالإضافة إلى ذلك الدليل عليه.

---

[499] د/ أحمد محمد محمود خلف، الحماية الجنائية للمستهلك، مرجع سابق، ص 199.

[500] المستشار/ معوض عبد التواب، الوسيط في شرح جرائم الغش والتدليس وتقليد العلامات التجارية، دار المطبوعات الجامعية، الطبعة الرابعة، 1998، ص20.

ثالثا: موقف المشرع الفرنسي من جريمة الإعلان المضلل: قد تم تجريم الإعلان الكاذب والمضلل في فرنسا بالقانون 2 قانون يوليو 1962، وقام بتنظيم القانون 1973/12/27 المعدل بالقانون 10 يناير 1978 ووسع مضمون جريمة الإعلان الكاذب أو المضلل، وكذلك حدد تقنين الاستهلاك الفرنسي الصادر في 1993/7/26 مفهوم الإعلان الكاذب والخادع والعقوبات التي تطبق عليه، فكل إعلان من شأنه أن يؤدي إلي الوقوع في غلط أو خداع بشأن الأموال والخدمات يكون محظوراً طبقاً لهذا القانون "والحق أن هذه الجريمة التي جرى تضمينها في المادة 1-121 من تقنين الاستهلاك قد تحولت إلي جنحة الممارسات التجارية المضللة، بموجب القانون الصادر في 3 يناير 2008.[501]

وأيدت محكمة النقض القرار الصادر عن قضاة الاستئناف بالآتي (ارتكب المتهمون الجنح المنصوص عليها 1-121، 121-18 و121-9 من تقنين الاستهلاك، الواجبة التطبيق من تاريخ حدوث الواقعة وتشكل ممارسات تجارية بعضها غير نزيه، والبعض جسيم بالمعنى الوارد في المادة 120-1 من تقنين الاستهلاك في الصياغة التي تمت بموجب قانون 4 أغسطس 2008 ، وذلك بفعل إيقاعها للمستهلكين في الغلط بشأن الخصائص الجوهرية للخدمات المقترحة.[502]

وفي الواقع أن المادة 120-1 ، التي جاء بها قانون 3 يناير 2008 ، والتي جرى تعديلها في 4 أغسطس التالي بموجب قانون IME ـ تعتبر نص عام ، يكرس لمجموعة من المبادئ الموجهة غير المشمولة بأي جزاء جنائي ثم أن هذه المادة ذاتها المنصوص عليها في تقنين الاستهلاك تعتبر مادة استهلالية في تقنين الإجراءات الجنائية [503].

الإعلان التجاري الخادع أو المضلل له صور عديدة يصل بها إلي المستهلك بما فيها النشر عبر الإنترنت، من ذلك حجب المعلومات الكافية عن المستهلك علي نحو يخل بحقه في الإعلام. مثل استخدام بعض المفردات التي تجذب المستهلك مثل الأقوى، الأوحد، المعجزة ... الخ .

فبالنظر إلي تنوع العناصر المنصوص عليها في المادة 1-121 من تقنين الاستهلاك نجد أن المشرع ، وضع فئتين للإعلان المضلل، على الرغم مما يوجد بينهما من تداخل في الواقع العملي، فالفئة الأولى، وهي المتعلقة

---

[501] C. Ambroise- Castérot,, Droit pénal de la consommation, Chron.Juris., RSC, 2010, P. 147.

[502] C. Ambroise - Castérot, - Castérot, Chron.,op. cit. P. 147.

[503] C. Ambroise - Castérot, Chron., op. cit. P. 148.

بوجود طبيعة وخصائص المال أو الخدمة المقترحة، أما عن الفئة الثانية، فإنها تتعلق بهوية، وجودة، وقدرات المعلن (فقد يكون المعلن صانع، أو بائع، أو مستثمر، أو ملتزم بعمل).

- ففي الفئة الأولى: يجدر الإشارة إلى عنصر هام، وهي ثمن السلعة أو الخدمة المقترحة ، وبناء عليه تقع جنحة الإعلان المضلل أو الذي يؤدي بطبيعته إلى الوقوع في الغلط [504]، كما في الأمثلة الآتية:

- حالة مدير شركة توزيع، الذي يقترح في إطار حملة دعائية، مواد عالية الجودة بأثمان مغرية لفترة محدودة، بينما لم يكن بعض المنتجات مهيأة خلال هذه الفترة بسبب عدم وجود بضاعة في المخازن[505].
- حالة الإعلان المسبوق بالنشرة التمهيدية عن تصفية كاملة والبيع بأثمان منخفضة لأجهزة كهربائية منزلية، بينما لا يشمل الثمن المنخفض سوى جزء صغير من هذه البضاعة.
- ونرى هنا أن القانون يجرم العروض التي تؤدي إلى الوقوع في الغلط حينما تنصب علي ثمن وشروط بيع الأموال، أو الخدمات، موضوع الإعلان .

- الفئة الثانية : أما عن الفئة الثانية للإعلان المضلل طبقاً للعناصر المنصوص عليها في صريح المادة 121-1 فهي تلك التي تتعلق بهوية وجودة وقدرات المعلن، ويمكن الرجوع إلي الأحكام القضائية التي صدرت بشأن هذه الفئة من الإعلان على وجه الخصوص، وعلى هذا النحو يتحقق بتحقق وصف جنحة الإعلان المضلل المنصوص عليها في المادة 1-121 من تقنين الاستهلاك على الحالات الآتية:

1- حالة المعلن الذي يقدم خدمة عقارية على النحو الذي يدعو إلى الاعتقاد بأنه موكل من عملاء أجانب للقيام بشراء عقارات، ومن حيث الواقع العملي ينحصر دوره في مجرد إرسال الملفات إلي الوكالات العقارية الأجنبية.[506]

2- حالة موزع الخمور عندما يستخدم صفة المالك الحاصد للكروم، بينما وفي مجاله الزراعي نجد أن لفظ المالك يعني الملكية العقارية ولفظ الحاصد تعني الشخص الذي يقوم بالزرع والحصاد لثمرة إنتاجه.[507]

---

[504] A Giudicelli, chroniques précite, op, cit. p. 117.

[505] Aix-en- provence, 15 jan , 1998, préc.

[506] Reim, 8 Jull, 1998, Juridata'm 43571.

[507] Bordeaut, 15 Janu, 1998, Préc.

3- كذلك في حالة قيام مدير شركة تبديل المنزل بالإعلان في الصفحات الصفراء - فرانس تيلكوم، حيث نوه في الإعلان أن شركته استفادت من العلامة "NF Service" بينما ومن الواقع العملي لم يكن يملك شهادة مطابقة.[508]

يضاف الى ذلك حالة أخرى في مجال الإعلان المضلل، وعلى غرار الحال بالنسبة للمجالات الأخرى، يجوز إعفاء مدير الشركة من المسؤولية متى يراهن على أنه فوض سلطاته لتابعه، وهناك العديد من القرارات التي تؤكد أن صحة التفويض رهن بأن سيتم للشخص الذي يملك الاختصاص، والسلطة، والوسائل الضرورية والتفويض يكون مقبولاً في ذات الشروط.

وقد أيدت محكمة النقض حكم محكمة استئناف Aix-en-provence، حيث قضت أن المستند المعنون بتفويض سلطات والذي قدم لأول مرة أمام محكمة الاستئناف ولم يتضمن وصف المفوض إليه، ولكن فقط مجرد توقيع مختلف عن التوقيع الموضوع على محضره الرسمي المصدر بالاستماع لدى البوليس لا يعفي المدير العام للشركة من المسؤولية الجنائية عن الإعلان المضلل[509] اعتبرت محكمة النقض الفرنسية[510] إعلان المهني عن النقل والتسليم خلال مدة قصيرة على الرغم من تمام ذلك خلال أسابيع متعددة بمثابة إعلان مضلل ويخضع نطاق التجريم.

وفي مجال التعاقد عن بُعد قضي بأن دور "إمداد المستهلك بمعلومات كاذبة أو غير صحيحة في كتالوج الشراء عن بُعد أمر يدخل ضمن الإعلان المضلل.[511]

وقد أيدت محكمة النقض الفرنسية هذا الإتجاه معتبرة أن إمداد المستهلك بمعلومات كاذبة أو غير صحيحة، يخفى علي مسلك المهني القيام بالإعلان المضلل عن منتجاته.[512]

كما نجد انه قد افرد نصوص جنائية واضحة تواجه الإعلان المضلل، فقد اهتم المشرع الفرنسي بالنص على جزاءات رادعة لهذه الجريمة وذلك في نص المادة 6/121 التي قررت تطبيق العقوبات الواردة في المادة

---

(508) Grenoble, 11 férr, 1998, Jurisdata'n o40886.

(509) Aix- en- provece, 15 Janu. 1998, Préc.

(510) Cass-Crim., 11 Déc 2007, ccc 2008, Comm. 125, Note : G. Raymond.

(511) Cass Crim., 17 Sept. 1997 ccc 1998. Comm. 125. Note : G. Raynnomd.

(512) Cass. Crim., 11 Déc. 2007 ccc 2008, Comm. 120. Note : G Raynnomd.

1/213 (عقوبة الحبس سنتين و الغرامة 250 فرنك أو إحدى هاتين العقوبتين)[513] ، لعقاب المسئول عن جريمة الخداع الإعلاني سواء كان طرفا في العقد أو ليس طرفا فيه وسواء حدثت الجريمة تامة أو جاءت في صورة المشرع فقط أيا كانت الصورة التي مارس من خلالها خداعه حتى و إن كانت عن طريق وسيط القضاء الفرنسي أعطى أهمية بالغة للمستهلك وحمايته من أي فعل يشكل خداع إعلاني فقد ساوى بين الشروع والجريمة التامة في العقاب لتشديد الخناق على الجاني.

1: **حظر الإعلان** [514] **:** في الواقع، وحتى عام 1963، لم تكن المحاكم تعاقب على الإعلان الكاذب، أو المضلل إلا مع النصوص الخاصة والتي نذكر منها، المادة 405 من القانون العقابي القديم المتعلقة بالنصب، والمادة الأولي من قانون الأول من أغسطس 1905 بشأن الغش. ولعل قانون 2 يوليو 1963 هو الذي عاقب بدوره على الإعلان المضلل، باعتباره أول قانون تناول هذه المسألة. ولكن لم يكن هناك بد من تغيير هذا النص، الذي كشف عن عدم جدواه وعليه فقد تناولت المادة 44 من قانون 27 ديسمبر 1973 الصادر تحت اسم قانون ***Royer*** هذه المسألة حيث نص على عقاب كل إعلان مضلل، وهنا نجد أن فكرة الإعلان المضلل أوسع من فكرة الإعلان الكاذب.

على هذا الحال، ومنذ عام 1973 أضحي لدينا جنحة الإعلان المضلل ***publicité trompeuse***. ومن نافلة القول، أن قوانين بعض الدول الأخرى بالإتحاد الأوروبي، قد سارت على هدي فرنسا من حيث فرض عقوبات ضد الإعلان المضلل أو الكاذب. بيد أن التعريفات والشروط، وكذلك الجزاءات تختلف من بلد إلي أخر.

وبالمقابل، هناك بلدان أخرى ليس لديها ثمة تشريع بخصوص هذه المسألة. ومن ثم، فلا غني عن تحقيق التناغم بين القوانين المختلفة لبلدان الاتحاد الأوروبي بشأن هذه المسألة. وهو ما تحقق من خلال التوجيه الأوروبي الصادر في 10 سبتمبر 1984[515] . والأمر هنا يتعلق بتوجيه أوروبي في الحدود الدونية له: فالدول لم تقدم القدر الكافي من الحماية للمستهلكين، فقد كان من الواجب عليهم منح المستهلكين قدر أكبر من الحماية في مواجهة الإعلان المضلل. ومن ناحية فرنسا، فإنها لم تبادر من جانبها بتعديل المادة 44 من قانون 1973، فهذا النص يكفل حماية مكافئة الحماية التي يتطلبها التوجيه الأوروبي.

---

[513] **J.-C. Auloy, F. Steinmetz, Droit de la consommation, 4e éd., Dalloz, 1996, P. 109.**

[514] **Buil, Sept ans de publicité mensongère, Cahiers de droit de l'entreprise 3-1981 ; Fabre, Publicité mensongère ou trompeuse, évolution récente de la jurisprudence, Cahiers de droit de l'entreprise 3-1983.**

[515] **Renaudiere, La directive 84/405 CEE sur la publicité trompeuse : la situation en Belgique, en France, au Royaume-Uni, en Irlande et aux Pays-Bas", RED consom. 1989.3.**

على أية حال، فقد تم إدخال المادة 44 من قانون 1973 في تقنين الاستهلاك حيث المواد من 121-1 إلى 121-7. وسوف نتناول بالشرح والتحليل هذه المواد من خلال دراسة الركن المادي لها، فضلاً عن ركنها المعنوي والعقوبة واجبة التطبيق. وسوف يتضح لنا فيما بعد كيف أن هناك نصوص أخرى واجبة التطبيق على موضوع الإعلان المضلل.

2: الركن المادي لجنحة الإعلان المضلل: تنص المادة 121-1 من تقنين الاستهلاك على : (" لا يجوز عمل الإعلان المتضمن، بأي شكل من الأشكال، لإدعاءات، أو بيانات، أو مزاعم، أو عروض غير صحيحة، أو تؤدي بدورها إلي الوقوع في الغلط، متى كانت تتعلق بواحد، أو أكثر من العناصر التالية :

وجود، وطبيعة، ومحتوى، والصفات الجوهرية، والمضمون، وكذلك الصــنف، والأصل، والكمية، والطريقة، وتاريخ التصنيع، والملكية، وثمن وشروط البيع للأموال، أو الخدمات، التي تشكل موضوع هذا الإعلان، وشروط استخدامها والنتائج المتوقعة من استخدام هذه الأموال، أو الخدمات، وأسباب، أو طرق البيع، أو الالتزام بالخدمات،...). في الواقع، إن هذا النص يكشف بدوره عن شروط ثلاثة يجب استيفائها حتى يمكن القول بوجود الجنحة [516]:

2-1: بداية، يجب أن يكون هناك إعلان ***publicité***. والإعلان بالمعنى الضيق للكلمة يعني الرسالة الموجهة إلي الجمهور في سبيل إنعاش الطلب على الأموال، أو الخدمات. ومن ناحية القضاء الفرنسي، فإنه لم يقصر عن تطبيق المادة 44 من قانون 1973 (المادة 121-1 من تقنين الاستهلاك)، حيث تبني تفسير واسع للفظ الإعلان، وبحسبه أن الإعلان يعني كل رسالة يقوم من خلالها أحد الأفراد بتعريف الجمهور بالأموال، أو الخدمات، التي يقترحها.

بيد أن الأمر يتعلق بمعلومة بسيطة دون أن ترتبط بغاية، أو هدف الحث على الشراء[517]. ولقد جرى توجيه النقد لهذا القضاء الواسع من جانب بعض الفقهاء[518]. ومن وجهة نظري، فإنني أري بوجوب تأييد هذا القضاء

---

[516] **J.-C. Auloy, F. Steinmetz, Droit de la consommation, op. cit., p. 110.**

[517] **على هذا النحو، فإن الكذب في البيان الإلزامي على التكيت يستوجب عقاب الإعلان المضلل،**

- Crime., 25 juin 1984, D. 1985.J.80, note Fourgoux

كذلك فإن الكذب في الإعلانات الحائطية له طابع بياني خالص:

Crim. 2 oct. 1985, RTD com. 1986. 541, obs. Hèmard et Bouloc.

[518] **انظر التعليق السابق السيد Fourgeoux**

ذاته. فأياً كان محتوى الرسالة الإيضاحية البسيطة، فإن النتيجة التي تترتب على الغش تكمن في جذب نظر المشترين. وطابع الغش، الذي تصطبغ به الرسالة البيانية، أو الإيضاحية يأخذ إذن طابع الإعلان.

على هذا النحو، يمكن تعريف الإعلان من حيث كونه يأخذ العديد من الأشكال المتباينة، التي تدخل في مجموعها في مجال تطبيق المادة 121-1 :

- تقع جنحة الإعلان المضلل، دون النظر إلى الدعامة التي تم نقل الإعلان من خلالها، حيث الصحف، أو الإذاعة والتلفاز، والإعلانات الحائطية، والتيكيت، إلى آخره،.....

- تقع الجنحة، أياً كان شكل الإعلان، سواء أخذ صورة المحررات، أو الأقوال، أو الصور.

- لا أهمية لما إذا كان الإعلان يتعلق بالمنقولات، أو العقارات، أو الخدمات[519].

- ليس لصفة المعلن ثمة أثر، فالإعلان يصدر بصورة عامة عن التاجر، أو الشركة التجارية، ولكن من الممكن أن تقع هذه الجنحة بطريق شخص غير تاجر ومن ثم يمكن أن تقع كذلك بطريق شخص غير محترف[520].

- لأهمية كذلك للأشخاص المعنيين بهذا الإعلان: المستهلكون، أو المحترفون وكافة اللذين يتمتعون بالحماية في مواجهة الإعلان المضلل[521].

في الواقع، إن الإعلان يشكل إذن عنصر ضروري حتى يمكن القول بوجود جنحة إعلان مضلل. ويجب أن تصدر الرسالة عن الشخص، الذي يسعى إلى إطلاع الجمهور على الأموال، أو الخدمات التي يقترحه[522]. ومن ناحية أخرى، يجب أن توجه الرسالة إلى جمهور المستهلكين:

---

[519] وفيما يتعلق بالتطبيق على العقارات، أنظر على سبيل المثال :

. Paris, 24 mai 1982 D. 1983.J.11, note Pradel et Paire

[520] تطبق محكمة النقض المادة 44 من قانون 1973 (المادة 121-1 من تقنين الاستهلاك) على الإعلان المضلل الصادر عن فرد عادي (Crim., 24 mars 1987, JCP, éd. E, 1988.II.15321, note Heidsick). ولم يرد لفظ المحترف في نص المادة 121-1 ولعلنا نتساءل ألا يتعارض الاتساع في مجال تطبيق المادة بحيث تشمل الأشخاص غير المحترفين مع روح النص.

[521] Crim., 2 oct. 1980 (D. 1981.IR.292 ; RTD com. 1981.619, obs. Bouzat.

[522] Aix, 13 févr. 1980 (D. 1980.J. 618, note Endréo.

على أي الحال، فإن المستند المقدم لشخص لا يعتبر في جوهره إعلان، ويجب أن يكون الغاية من الرسالة الإعلانية الحث على إبرام عقود في المستقبل بشأنها. والمستند المستخدم عقب إبرام العقد، لا يعتبر في جوهره إعلان[523].

2-2: إن طابع الغش في الإعلان يشكل إذن عنصر جوهري في الجريمة. ووجد هذا العنصر لا يثير ثمة شك حينما تنطوي الرسالة على غش ظاهر بطريق الكتابة. وعلى هذا الحال، فإن العقاب يطال الإعلان الذي يبلغ عن منتج بدون صبغة، بينما يتضمن المنتج صبغة.

ولكن المادة 121-1 لم يأخذ ذلك في الاعتبار. حيث تعاقب هذه المادة كل إعلان يؤدي بطبيعته إلى الإيقاع في الغلط[524]. فالأمر إذن يتعلق بالإعلان الإيحائي ***la publicité suggestive*** الذي يهدف إلى إيقاع جمهور العملاء في الغلط. كما هو الحال على سبيل المثال في حالة المشروب الذي يحتوي على مواد كيميائية، ويقدم للجمهور على أنه مشروب بطعم الفواكه، ففي هذه الحالة نجد أن المعلومة صحيحة في حد ذاتها، ولكن متى صاحب عرض المنتج صورة للفواكه الطازجة، فإنها قد تدفع بالمستهلكين إلي الاعتقاد بأن المشروب مصنوع من الفواكه الطازجة، وهو غير صحيح[525].

على هذا الحال، يتحتم منع الغش بطريق الإيحاء، حيث يكثر اللجوء إليه ولا جرم في أنه أكثر خطورة من الغش بطريق الكتابة.

ومن ناحية القضاء، فقد وضع بدوره حدود على العقاب، على نحو ما يبين المثال التالي. ففي سبيل التدليل على متانة حقيبة، عرض الإعلان عبر التلفاز جزء من الكرة الحديدية للبلدوزر للإيحاء بقوة الحقيقة ومتانتها. وقد تم تمرير هذا الإعلان مرات عديدة في نماذج البلدوزرات.

---

[523] على هذا النحو، فإن الخطاب المرسل إلي مشتري بطريق البائع لوصف المال المبيع، ولكن الخطاب جرى تحريره من خلال نسخ عديدة، وجرى إرساله إلى سلسلة من العملاء الاحتماليين، مما يعني أنه أخذ طابع الإعلان :

-Crim., 21 mai 1974, D. 1974.J.579, rapport Robert.

[524] هناك صيغة مماثلة في التوجيه الصادر بتاريخ 1984 : (" الإعلان الذي يوقع في الغلط، أو الذي يمكن أن يؤدي إلي الوقوع في الغلط ").

[525] Affaire Tang : Crim., 13 mars 1979 (JCP, éd. Cl, 1979.I.13104)

نستطيع الاستشهاد بقضية News : حيث يتحقق وصف الإعلان المضلل، الذي يوقع في الغلط، على استخدام اللغة الإنجليزية لتقديم سجائر في علب للسجائر بفرنسا

هنا تم رفع دعوى الغش بطريق الإعلان المضلل ضد المعلن[526]. ولكن من المستحيل بطبيعة الحال، أن يكون للحقيبة متانة وقوة الكرة الحديدية للبلدوزر، ومن ثم فقد قضت محكمة أول درجة لصالح المعلن بالبراءة، لأن الإعلان لم يكن ليؤدي بطبيعته إلي إيقاع العميل في الغلط. ونقصد هنا على الأخص المستهلك العادي القادر على فهم المغذي من الرسالة الإعلانية[527].

وهنا يعن لنا أن نتساءل عن فئة الأشخاص، الذين يمكن أن تحيل عليهم المحاكم لمعرفة ما إذا كان الإعلان يؤدي من عدمه إلي الإيقاع في الغلط ؟

هنا يمكن الوقوف عند نموذج الشخص العادي في القانون المدني. ولكن متى أخذنا بمثل هذه المرجعية في القانون المدني، فلا جرم في أن ذلك سوف يؤدي بدوره إلي تجريد المادة 121 من تقنين الاستهلاك من فعاليتها.

والتطبيق لهذا المبدأ المستقر في القانون المدني، أن المعول عليه هو المستهلك العادي، أو المتوسط. ولكنه أقل قوة من الحال بالنسبة للشخص العادي في القانون المدني، مما يعني تراجع مستوى الحماية. ومن الملاحظ، أن بعض الإعلانات توجه إلي مجموع المستهلكين، وهناك فئة خاصة من المستهلكين، وفئة أخرى من المحترفين. ومثل هذه الرسالة الإعلانية، التي لا توقع المحترف في الغلط، لن توقع كذلك المستهلك العادي المعني بالحماية.

ويبدو أن هذه الرسالة تقع تحت طائلة المادة121-1، فليس من الضروري أن يكون الإعلان ذاته قد أدي إلي الوقوع في الغلط. ولكن يكفي أن يؤدي بطبيعته إلي ترتيب مثل هذا الأثر[528]. والمعلن الذي قام بنشر إعلان كاذب، أو أدي إلي الوقوع في الغلط، لا يمكن أن يؤدي إلي الإفلات من العقاب لمجرد قيام المعلن بنشر معلومات حقيقية[529]. والجنحة المنصوص عليها في المادة 121-1 تعتبر إذن جنحة وقتية:

Le délit instantané.

---

[526] J.-C. Auloy, F. Steinmetz, Droit de la consommation, op. cit., p. 111.

[527] Affaire Samsonitté : Crim., 21 mai 1984 (D. 1985.J.105, note Marguery ; RTD com., 1985.379, obs Bouzat.

[528] Crim., 8 déc. 1987 (D. 1988.IR.43).

[529] Crim., 30 mai 1989 (D. 1989.IR. 226 et 246.

بينما وفيما يتعلق بمقدار العقوبة، يمكن للقضاة أن يأخذوا في الاعتبار الجهود المبذولة من المعلن في سبيل محو الآثار المترتبة على الرسالة المنطوية على الغش.

3-2: أما عن الشرط الثالث، فإنه يتمثل في الآن الإعلان المضلل لا يستوجب العقاب إلا متى انصب على احد العناصر المنصوص عليها في المادة 121-1[530] . والحق أن هذا الشرط يكفي على غرار مستوى العناصر السابقة. ومن المتصور أن الإعلان يستوجب الجزاء لمجرد كونه مضللا. والحق أن العناصر السابقة متعددة، وعليه فسوف نحاول تصنيفها على النحو التالي:

- إن الإعلان المضلل يستوجب العقاب متى تعلق بمال، أو بخدمة، وهو ما تواتر عليه الحال[531].
- كما أن الإعلان يستوجب الجزاء حينما ينصب بدوره على شروط البيع، أو الخدمة المقترحة، وعلى وجه الخصوص على ثمنه[532].
- كذلك يلزم العقاب ضد الإعلان الذي يترتب عليه الوقوع في الغلط بشأن شخص الصانع، أو البائع، أو متعهد الخدمة[533].

صفوة القول، إن العناصر التي يعتمد عليها الإعلان المضلل، والتي يكون على أساسها مستوجب للعقاب، من التعدد بحيث أن من الصعوبة بمكان الإحاطة بها. ولقد تمسك المشرع بالشرطي الأول والثاني. ومن ثم فإنه لم يجد ثمة بد من السير في هذا الطريق.

على هذا الحال، تنص المادة 3 من التوجيه الأوروبي الصادر في 10 سبتمبر 1984 على: (" إن الإعلان المضلل يرتكز على مجموعة من العناصر"). ومن ناحية المشرع، فإنه لم يقصر من جانبه عن محو الطابع الحصري.

---

[530] إن حكم محكمة الاستئناف، الذي لم يبين أن الإعلان المضلل واقع على أحد العناصر المنصوص عليها في المادة 121-1 يستوجب نقضه.

- Crim., 28 mars 1984, D. 1984.IR. 390.

[531] على سبيل المثال الإعلان، الذي يقدم مشروب يحتوي على مواد كيميائية على أنه مشروب طبيعي

Crim., 13 mars 1979, JCP, éd. Cl, 1979.I.13104, Chron. Guinchard

كذلك الحال، بالنسبة للإعلان الذي يدفع إلي الاعتقاد بأن الفعالية العلاجية للمنتج مضمونة بالتصديق الرسمي على ذلك.

[532] Crim., 3 sept. 1992, JCP, éd. E, 1992.Pan.1237.

[533] CRim., 15 févr. 1982, D. 1983.J.275, note Mayer et Pizzio.

3: الخطأ، أو الإهمال، باعتباره عنصر في جنحة الإعلان المضلل: إن القانون الأول المتعلق بالإعلان الكاذب يتمثل في قانون 2 يوليو 1963، الذي جعل من سوء النية ركن في الجريمة. فالفاعل لا يستوجب العقاب، إلا متى قصد إيقاع المستهلك في الغلط. بينما ألغي قانون 27 ديسمبر 1973 في مادته 44 الإحالة على سوء النية. وخلال اليوم التالي، لإعلان هذا القانون، استند البعض من الفقهاء على أن صمت القانون لا يكفي لاستبعاد مقتضى الركن المعنوي[534].

والحق إن محكمة النقض لم تقبل بهذا التفسير، حيث قضت بأن سوء النية لا يعتبر ركن في جريمة الإعلان الكاذب[535]. ومنذ اللحظة التي يتكون فيها الركن المادي للجريمة، فإن المعلن يستوجب العقاب، حتى وإن لم يثبت لديه سوء نية. وفي عام 1073، جرى استبدال جنحة الإعلان الكاذب بجنحة أوسع، وهي الإعلان المضلل.

ومن الملاحظ، أن قضاء محكمة النقض لم يخرج عن مقاصد المشرع في عام 1973. وفي ظل قانون 1963، لم يكن عقاب الإعلان الكاذب يكفي لكون المعلنين اللذين نشروا إعلان كاذب كانوا في الغالب يدعون بأنهم لم يكونوا سيئ النية. ومن ناحية أخرى، كان من المستحيل التدليل على سوء النية. بينما جاء قانون 1973 ليوسع بدوره من التجريم. ومن ثم فلم يكن في إمكان المعلنين التخفي وراء الإهمال والتذرع بالخطأ.

ويمكن أن يُحكم على الشخص المعنوي مثل الشخص الطبيعي جنائيا لإعلان كاذب أو قد يؤدي الى غلط، إذا لم يتحقق من صحة ما ذكر، وجنحة الإعلان الكاذب ما هي ثمرة سياسة وتجارية مرغوبة ومنظمة من قبل الشخص المعنوي، يمكن إدانته حتى ولو لم يكن هناك إمكانية لنسب الجنحة لهيئة أو لممثل قانوني معين، في النهاية قضت محكمة النقض الفرنسية بالحكم على المتهم بغرامة قدرها 70 ألف يورو، فأن محكمة الاستئناف قضت وفق مقتضيات المادة 121 – 6 من قانون الاستهلاك، وكذا المادة 131 – 38 من القانون الجنائي، والتي بمقتضاها الحد الأقصى للغرامة المطبقة على الأشخاص المعنوية تساوي خمس مرات الغرامة المطبقة على الشخص الطبيعي[536].

---

[534] Fourgoux, " La publicité mensongère, délit intentionnel ", Gaz. Pal. 1977.I. Doct. 76.

[535] Crim., 4 déc. 1978 (D. 1979.IR. 180, obs. Roujou de Boubée.

[536] Crim. 24 mars 2009, n° 08-86530, CCC 2009, comm. 235, obs. Raymond ; Dr. pénal 2009, comm. 84, obs. Robert.

تجدر الإشارة أن هناك قرار آخر في آخر نفس السنة (15 ديسمبر 2009) قضى بأن فعل الخداع يقتضي جنائي، وعاد بذلك لصريح نص مقتضيات المادة 121 - 3 من مدونة القانون الجنائي الفرنسي.

4: الركن المعنوي لجنح الإعلان المضلل، والتي أضحت تحمل وصف الممارسة التجارية المضللة **l'élément moral du délit de publicité trompeuse, devenu pratique commercial trompeuse.**

إن المشكلة الثانية التي أثارها هذا الحكم تكمن في معرفة طبيعة الركن المعنوي للجريمة المنصوص عليها في المادة 121-1 من تقنين الاستهلاك. وبالمقابل، فإن الجواب الذي جاءت به الدائرة الجنائية بمحكمة النقض ينطوي على شيء من الابتكار. وفي عام 1963، اقتضت هذه الجنحة توافر حسن النية، وهو المقتضى الذي ظل مطبقاً خلال ما يزيد على العشرة أعوام، حتى مع قانون 27 ديسمبر 1973. حيث كان السؤال في البداية يثور حول حسن، أو سوء نية المعلن، ثم أصبح هذا السؤال بعد ذلك خارج الموضوع، ومن ثم فقد استقر الحال على الحكم ضد المحترف .[537]

بعد ذلك، أضحت هذه الجنحة غير متعمدة، وعقب صدور التقنين العقابي الجديد (الساري التطبيق في الأول من مارس 1994)، ثم ما لبثت محكمة النقض أن عاودت تأييد هذا الحل، وقد استندت في ذلك على أحكام المادة 339 من القانون رقم 92-1336 الصادر في 16 ديسمبر 1992، الذي يحمل اسم " قانون تكييف التقنين العقابي الجديد" .[538]

على هذا النحو، يكفي الخطأ البسيط الناجم عن الرعونة، أو الإهمال[539]. ومن ثم فلم تنفك الدائرة الجنائية بمحكمة النقض عن الحكم بأن، (" إن إهمال المعلن، الذي لم يتحرى الصدق والحقيقة في الرسالة الإعلانية المجرمة قبل نشرها، يميز الركن المعنوي لجنحة الإعلان المضلل")[540] .

إن هذه الجنحة الشكلية[541]- بحسب القضاء-، تعتبر غير متعمدة. فالرعونة، أو الإهمال، أو عدم التبصر، كلها صفات تميز الركن المعنوي للجريمة. ومن ثم فإن منطق قضاة الموضوع يرتكز في الأساس على المحترف

---

(537) Crim. 4 déc. 1978, D. 1979. IR. 180, obs. G. Roujou de Boubée.

(538) Crim. 14 déc. 1994, Bull. crim. N° 415.

(539) Crim. 19 oct. 2004, Bull. crim. N° 245.

(540) Crim. 12 nov. 1997, Dr. Pénal 1998, comm. 24, obs. Robert.

(541) Ph. Cont, note sous Crim. 14 oct. 1998, JCP 1999.

الصالح، أو الشريف الذي لا يرتكب مثل هذه التصرفات الإيجابية، أو السلبية، وهو ما كان يعطي المبرر للحكم ضدهم.

وبالمقابل، متى تعمقنا النظر في الإرادة العقابية، ومن منظور الشرعية، فإن التسبيب قد لا يكون كاملاً. وبحسب المبدأ المنصوص عليه في المادة 121-3 الفقرة الأولي من التقنين العقابي، " لا جناية، أو جنحة ما لم تثبت نية ارتكابها". والقول بوجود جريمة الخطأ، أو الإهمال، يقتضي أن يكون القانون قد نص صراحة على هذا المضمون الخاص للركن المعنوي. ففي جريمة الإعلان المضلل، والتي أضحت الممارسة التجارية المضللة، لم يتم عمل أي تنويه بشأن الركن المعنوي لهذه الجريمة في صريح نص المادة.

بناءً عليه، وبحسب المادة 121-3 من التقنين العقابي، التي كانت موضوع للعديد من التفسيرات المركبة، إن الجريمة المنصوص عليها في المادة 121-1 من تقنين الاستهلاك يجب أن تنضوي تحت وصف الجنح المتعمدة،... وهو ما قضت به صراحة الدائرة الجنائية بمحكمة النقض في 15 ديسمبر 2009.

وفي سبيل الحكم ضد المتهم بجنحة الإعلان، الذي يوقع بطبيعته في الغلط استندت محكمة الاستئناف في قرارها على أن رئيس الشركة، ومنذ إنشائها لم يكن ليجهل الالتزام بتبصير المستهلك الواقع على كاهله بشأن تعريفات الخدمات المقترحة ولا بالطابع الكاذب للدعاية التي تنشرها شركته الخاصة.

على أية حال، فقد حاول المتهم النعي باللائحة على مثل هذا التسبيب مدعياً بأن هذا التسبيب يعود في الواقع إلي قلب عبء الدليل، حيث الجدل الكلاسيكي بشأن الركن المعنوي للجريمة[542]. والجواب الذي جاءت به محكمة النقض لم يكن متوقع. ومع تأييدها لحكم قضاة الموضوع، فقد استندت في تسبيبها على الفقرة الأولي من المادة 121-3 من التقنين العقابي المتعلقة بالجرائم المتعمدة، ومما جاء في حيثيات الحكم، نذكر ما يلي، (" وحيث أنه، وبالنظر إلي موضوع القضية، فإننا نستنتج، أن المتهم لم يكن قد اتخذ كافة الاحتياطيات الخاصة التي تضمن صحة الرسائل الإعلانية، وعندئذ ومع ثبوت المخالفة للضوابط القانونية واللائحية مع تحقق

---

[542] **أنظر تعليق :**

R. Saint-Esteben et J.-D. Bretzner, La charge de la preuve en matière de publicité trompeuse ou de nature à induire en erreur, D. 2006. 1610.

- كما انظر الجديد في جريمة النصب في قانون العقوبات الفرنسي الجديد لدى د/ محمد أبو العلا عقيدة، الاتجاهات الحديثة في قانون العقوبات الفرنسي الجديد، مرجع سابق، ص127.

العلم بذلك، فقد توافر القصد الجنائي لدى الفاعل، وهو المنصوص عليه في المادة 121-3 الفقرة الأولي من التقنين العقابي، وعليه فإن محكمة الاستئناف تكون بذلك قد بررت حكمها").

لأول مرة، بحسب علمنا تطبق الدائرة الجنائية بمحكمة النقض جنحة الإعلان المضلل المنصوص عليها في المادة 121-1 من تقنين الاستهلاك، والتي أضحت الممارسة التجارية المضللة، حيث اقتضت إثبات القصد الجنائي. والحق أن هذا الحكم واضح ولا ينطوي على أي غموض.

على أية حال، فقد آخذ على المتهم قصده الجنائي، والنص الذي كرّس لهذا الحل يتمثل في الفقرة الأولي من المادة 121-3 من التقنين العقابي. والحق إن هذا الخيار منطقي، وعقلاني ومن ثم يجب أن يحظى بالتأييد : الممارسة المنطوية على الغش، على غرار الحال بالنسبة لجرائم الغش (المادة 213-1 من تقنين الاستهلاك) أو النصب (المادة 313-1 من التقنين العقابي)، التي ترتكز على إرادة الجاني. والحق أن هذا المنطق يوافق الفكرة العامة للنزاهة التي يجب أن تتوافر في الشخص المحترف.

على أية حال، فقد أدخلت محكمة النقض، منذ بداية العام جنحة الإعلان المضلل في فئة الجنح غير المتعمدة، دون النظر إلي التعديل المزدوج الذي تم في عام 2008. بينما وفيما يتعلق بالممارسة التجارية المضللة، فقد أكدت الدائرة الجنائية بمحكمة الجنايات على أنه لا يوجد ثمة تغيير في تفسير وتقدير الركن المعنوي للجريمة.

أما بالنسبة للتوجيه الأوروبي:

فقد عرفت الإعلان الكاذب والمضلل في المادة الثانية من التوجيه الأوربي رقم 450 الصادر 1984/09/10 والتوجيه الصادر رقم 114 في تاريخ 2006/12/17 بأنه " إعلان بأي وسيلة من وسائل الإعلان يتضمن تضليله في بيان يؤدي إلي إيهام الشخص الموجه له الإعلان وذلك بمدة ببيانات خاطئة وتؤثر على سلوكه الاقتصادي بدفعه إلى التعاقد، والتي تؤدي إلي الإخلال بقواعد المنافسة ولم تضع المنظمة الدولية للتعاون الاقتصادي تعريفاً محدداً للإعلان التجاري، ولكنها عرفته في إطار الممارسات، وقد حددت بأن تكون تلك الممارسات التجارية مضللة عندما تؤدي إلي إيذاء المستهلك عن طريق تضليله بخصائص السلعة أو الخدمة أو طبيعتها أو شروط التعاقد [543].

[543] **القواعد الإرشادية للمنظمة الدولية للتعاون الاقتصادي Oecd لسنة 2003، والمنشورة على موقعها الالكتروني:**
www.oecd.com

الخاتمة

فى النهاية لا يمكننا أن ننكر بعد كل ما سبق، أن المستهلك الالكتروني ليس فرد او عدد محدود من الناس بل أصبح العالم كله مستهلك، وبالتطور التكنولوجي أصبح الغالبية العظمى من الأشخاص الطبيعيين والأشخاص الاعتبارية مستهلك إلكتروني، يستخدم الوسائل التقنية فى الحصول على كل ما يشبع حاجاته الشخصية والعائلية، ولهذا كان لابد من مواجهه او صوره من صور الاعتداء المستهلك، ألا وهي الإعلان الإلكتروني الخادع والمضلل للمستهلك والذي دائما ما يكون غرضة الاعتداء على حق من حقوق المستهلك الإلكتروني.

وقد خلصنا من هذة الدراسة الى نتائج، و توصيات نبرزها فيما يلى:-

أولا: النتائج:

- نتج من هذه الدراسة إلى أن مصر قد عرفت حماية المستهلك التقليدى منذ القدم،فكان لحماية المستهلك نظاما قانونيا على مر العصور، إلا أنها أصبحت على بداية الطريق نحو حماية المستهلك الإلكتروني، ذلك بعد صدور القانون رقم 181 لسنة 2018 بشأن حماية المستهلك المصري.
- على الرغم من حداثة التشريعات فى مواجهة جرائم الإعتداء على المستهلك الإلكتروني إلا أنها تحاول ساعية لمواجهة تلك الجرائم، والدليل على ذلك هو صدور القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات.
- إن جرائم الإعتداء على المستهلك الإلكتروني هي كل نشاط إجرامي يستخدم الإنترنت في ارتكابه، يكون الهدف من هذا الإجرام إستهداف حقوق المستهلك الإلكتروني، يلعب الإنترنت دور الوسيط في حصول المستهلك على ما يرغب به، كما يلعب دور الوسيط في الجريمة المعلوماتية .
- من الخطأ القانوني والتقني، قصر جرائم الإعتداء على المستهلك الإلكتروني في صورة واحدة أو شكل إجرامي واحد، فكلما تطورت النظم الإلكترونية، فكلما تطورت أشكال وصور جرائم الإعتداء على المستهلك الإلكتروني، فالعلاقة التي تجمع التجارة الإلكترونية والجرائم المعلوماتية هي علاقة طردية على الدوام.

- تتسم جرائم الإعتداء على المستهلك الإلكتروني بخصائص تقنية خاصة، تمثلت في صعوبة الإكتشاف، كما صعوبة الإثبات، كما السرعة الفائقة في ارتكاب هذا النوع من الإجرام، كما سهولة ارتكابها وطمس معالمها وأدلتها ومحو أثارها بسهولة وسرعة، دون ترك أثر ملموس.
- توصلنا في هذه الدراسة إلى أنه لابد أن تتسم قوانين مكافحة الجريمة المعلوماتية وحماية المستهلك الإلكتروني، بالمرونة والتقدمية لمواكبة التطورات التقنية والتكنولوجية المستمرة كل يوم، فالتكنولوجيا كل يوم في جديد، لابد أن يعادل ذلك تطور تشريعي هو كل يوم في جديد ايضا. فلا يوجد خبير قادر على التعامل مع كافة أنماط جرائم الإعتداء على المستهلك الإلكتروني.

ثانيا: التـــوصـيات:

في سبيل وضع أسس وركائز الحماية الجنائية للمستهلك الإلكتروني للوصول لأقصى درجات الحماية الموضوعية والإجرائية للمستهلك الإلكتروني، وبث الثقة في نفوس المستهلكين والمتعاملين عبر الشبكة العنكبوتية لتؤدي دورها المنشود على أكمل وجه نوصي بجملة من التوصيات على النحو التالي:

- نوصي بضرورة التنسيق بين الكيانات التي تتناول قضايا حماية المستهلك الإلكتروني، فتتجلى أهمية وضرورة التنسيق بين هذه الأطراف في بيئة تعددية تتداخل فيها الممارسات وتتطور في المنطقة نفسها. وتختلف أساليب تحقيق هذا التنسيق باختلاف البلدان. ومن المهم تحليلها وتحديد تلك التي تعمل على أفضل وجه لتوجيه البلدان الأخرى في الاتجاه الصحيح.

- نوصي بتفعيل دور الهيئات التنظيمية الوطنية القائمة على حماية المستهلك الإلكترونى، فتنطوي مسؤولية هذه الهيئات، على وضع إجراءات مناسبة لتلقي الشكاوى وتوجيه مطالبات المستهلكين، وتعريفهم بحقوقهم وحمايتهم في حالة حدوث خلل في السوق الإلكتروني. ففي غالبية البلدان، تتحمل الهيئات التنظيمية مسؤولية التعامل مع الشكاوى المقدمة من المستهلكين.

- نوصي بإنشاء كيانات مستقلة متخصصة تتعامل مع شكاوي المستهلك، ففي البرازيل هنالك ثلاثة كيانات تعمل مع الهيئة ANATEL للتعامل مع شكاوى المستهلكين. ويتلقى المكتب شكاوى المستهلكين من المشغلين أو منANATEL. وترسل الشكاوى بشأن المشغلين في بادئ الأمر إلى الخدمة المختصة (المشغل) الذي عليه أن يتصل بالمستهلك خلال خمسة أيام، وترسل الشكاوى بشأن الهيئة ANATEL إلى الإدارة المعنية موضوع الشكوى. ويوفر المجلس قناة اتصال بين ANATEL والجمهور ويقدم المعلومات ذات الصلة بأنشطة

ANATEL. وتتألف لجنة حماية مستعملي خدمات الإنترنت من ممثلين عن ANATEL والوزارة والمشغلين والمستهلكين، وتقدم المشورة إلى مجلس الإدارة بشأن حماية المستهلك. وقد وضعتANATEL أيضاً مؤشر الاهتمام بالمستهلك (IDA) الذي يحتوي على مزايا من حيث أنه أداة تطبيقية لتحسين حماية المستهلك في بيئة دولية متقاربة.

قائمة بأهم المراجع القانونية العربية

1) د/ أبو العلا النمر، المشكلات العملية والقانونية في التجارة الإلكترونية، دار النهضة العربية، 2004.

2) د/ أحمد محمد محمود الرفاعى، الحماية المدنية للمستهلك إزاء المضمون العقدي، دار النهضة العربية،1994.

3) د/ أسامة أحمد بدر، حماية المستهلك في التعاقد الإلكتروني، الطبعة الأولى، جامعة الإسكندرية، دار الجامعة الجديدة للنشر، 2005.

4) د/ السيد محمد السيد عمران، حماية المستهلك أثناء تكوين العقد، دراسة تحليلية وتطبيقية للنصوص الخاصة بحماية المستهلك، منشأة المعارف، الإسكندرية، 1986.

5) د/ أمنية خبابة، التحكيم الالكتروني في التجارة الالكترونية، دار الفكر والقانون، المنصورة 2010.

6) د/ جميل عبد الباقي الصغير:

- الإنترنت والقانون الجنائي، دار النهضة العربية، 2002.
- القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، دار النهضة العربية، الطبعة الثانية، 2012.

7) د/ خالد ممدوح إبراهيم، حماية المستهلك في المعاملات الإلكترونية، الدار الجامعية، الإسكندرية، 2007.

8) د/ سيد أحمد محمود، دور الحاسب الإلكتروني أمام القضاء، دار النهضة العربية، مصر، 2008.

9) د/ عبد الفتاح بيومي حجازي:

- النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، .2002
- حماية المستهلك عبر شبكة الإنترنت، الطبعة الأولي، دار الفكر الجامعي، 2006.

10) عبد الله ذيب محمود، حماية المستهلك في التعاقد الالكتروني، دراسة مقارنة، دار الثقافة، عمان، الطبعة الأولى، 2012.

11) د/ عبد المنعم زمزم، قانون التحكم الإلكتروني، دار النهضة العربية، 2009.

12) عبد المنعم موسى إبراهيم، حماية المستهلك، الطبعة الأولى، بيروت، منشورات الحلبي الحقوقية، 2007

13) د/ علاء عبد الباسط خلاف، الحماية الجنائية لوسائل الاتصال الحديثة، دار النهضة العربية، 2002.

14) 50) د/ عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، الطبعة الأولى، .2004.

15) د/ فريد منعم جبور، حماية المستهلك عبر الانترنت ومكافحة الجرائم الإلكترونية، دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الأولى،.2010

16) د/ محمد الحسني، حماية المستهلك الالكتروني في القانون الدولي الخاص، دار النهضة العربية، 2013.

17) د/ محمد طارق عبد الرؤوف الخن، جريمة الإحتيال عبر الإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، 2011.

18) د/ مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، الطبعة الأولى، 2001.

19) د/ هدى حامد قشقوش:

- جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، 1993.
- الإعلانات غير المشروعة في نطاق القانون الجنائي، الطبعة الأولى، مصر، دار النهضة العربية 1998.

ظاهرة التحرش والتنمر الرقمي

ليندا عماد عواد

باحثة في الشؤون القانونية والأمنية

الملخص:

في عالمنا المعاصر يوجد العديد من الضحايا للجرائم التي يتم ارتكابها من خلال شبكة الإنترنيت ووسائل التواصل الاجتماعي المرتبطة بها والتي يُطلق عليها عادة الجرائم الإليكترونية أو السيبرانية، أو غير ذلك من المسميات. وتهدف هذه الدراسة إلى التركيز على توعين من تلك الجرائم ألا وهما: التحرش الجنسي الإليكتروني والتنمر الإليكتروني. وبالرغم من أن هذه الجرائم وجدت من قبل فإنه تم استنساخها في عصر الإنترنيت. وفي واقع الأمر قامت العديد من الدول بسن قوانين للتعامل مع جرائم تكنولوجيا المعلومات، بما في ذلك التحرش والتنمر الإليكتروني، فإن الأمر يستلزم اتخاذ المزيد من الخطوات على مستويات مختلفة للتخلص من هذه الآفات الإليكترونية التي أضحت تحاصر العديد من الأشخاص، خاصة النساء والفتيات، في عصرنا الحالي. ومن ثم فإن هناك حادة إلى نشر الوعي الاجتماعي بمخاطر هذه الجرائم وطرق تجنبها، كما يلزم أن تقوم المدارس بدور هام في متابعة هذه التصرفات، أما بالنسبة للعائلة فيقع عليها عب التوجيه والنصح والإرشاد. وتهدف كافة هذه الإجراءات إلى مكافحة هذه الجرائم وتجنب تبعاتها السلبية الخطيرة ليس فقط على ضحاياها ولكن أيضاً على المجتمع ككل.

Résumé:

Cyber sexual harassment and Cyberbullying phenomena

In today's society, there are several ways in which people are victimized due to the use of the Internet and social media. This study focus on two bad methods of using the Internet namely: Cyber sexual harassment and Cyberbullying. These two forms of crimes already existed in our physical world. However, the advent of the Internet era has created a modern form of both of them. In fact, we are dealing with full crimes and many countries adopted laws to deal with the internet crimes including the abovementioned two. But this action, per se, is not enough to get rid of such crimes. Social awareness, school follow up, and family control should be encouraged to combat such crimes and to avoid its huge negative impact not only on the victims but also the society as a whole.

مقدمة

شهد العالم من قيام الثورة الصناعية، بمختلف مراحلها، تقدماً وتطوراً ضخماً في كافة القطاعات ومجالات الحياة، فقد نتج عن التطور المستمر في التكنولوجيا ظهور المزيد من الاختراعات والاكتشافات التي سرعان ما حولت العالم إلى قرية صغيرة يسهل التواصل بين مكوناتها بشكل فوري دون الحاجة إلى الانتقال الملموس أو الحصول على تأشيرات دخول أو اظهار جوزات السفر أو بطاقات التطعيم الصحية أو غيرها. وقد تبلور هذا التطور على وجه التحديد مع المرحلة الثالثة للثورة الصناعية، التي أطلق عليها مصطلح تكنولوجيا المعلومات.

على الرغم مما قدمه هذه التطور من مزايا لا حصر لها فإنه حمل في طياته أيضاً جانباً مظلماً فتح الطريق أمام العناصر الإجرامية لاستخدامه في ارتكاب العديد من الجرائم التي اتسمت بطابع الحداثة وإن وجد مثيلها في الواقع الفعلي، وهكذا ظهرت مصطلحات جديدة من قبيل الجريمة الإليكترونية أو الجريمة الرقمية والتي تتخذ من الفضاء الافتراض مسرحاً لها، ويكون كل من الجاني والضحية من الأشخاص الطبيعيين ولكن ذو صفة رقمية تمكنهم من استخدام المنصات الاليكترونية. في ضوء صعوبة تناول كافة أنواع الجرائم الرقمية في ورقة بحثية محددة، فإننا سنقتصر فقط على تناول كل من ظاهرتي التحرش الجنسي والتنمر الإليكتروني.

تلزم الإشارة، في البداية، إلى أن الجريمة كواقع مجتمعي تتطور بتطور الزمان والمكان، فهي ظاهرة اجتماعية قديمة ومستمرة، ومع التطور التقني ظهرت الجريمة الإليكترونية؛ التي تُعتبر ظاهرة إجرامية مُستحدثة تستهدف المعطيات بدلالاتها التقنية الواسعة، سواء تعلق الأمر ببيانات أو معلومات أو برامج، وكذلك القيم التي عرفتها المجتمعات بمختلف أنواعها. وفي هذا السياق، تعددت أبعاد وصور ا لجريمة الإليكترونية. ويُشار في هذا الخصوص إلى أنه نتيجة للاستخدام المستمر والمتزايد لوسائل التكنولوجيا بأشكالها المتعددة:

كالهاتف النقال، والبريد الإليكتروني، والمواقع الإليكترونية، فضلا عن خاصية البلوتوث ومواقع التواصل الاجتماعي والمنتديات التي يرتادها بشكل دائم ومستمر الشباب والفتيات في عصرنا الحالي، أضحت هذه المواقع مجالاً خصباً لانتشار عدد من أشكال الجرائم الإليكترونية في مقدمتها التحرش الجنسي الإليكتروني والذي يُعتبر امتداد للتحرش الجسدي الذي سبقه في الانتشار على أرض الواقع بشكل يدق ناقوس الخطر.

وتمثلت المحصلة النهائية لذلك في معاناة الكثيرين من مستخدمي الأجهزة الاليكترونية المتصلة بشبكة الإنترنيت من العديد من الجرائم الإليكترونية بشكل عام، والتحرش الجنسي بشكل خاص من خلال تعرضهم

للمضايقات بأشكال مختلفة، من قبيل الملاحقة بمختلف مستوياتها، كما أن البعض قد يتعرض لظاهرة التنمر الاليكتروني، بما تعنيه كل من الظاهرتين من آثار سلبية على شخص المجني عليه.

أهمية الدراسة:

تتسم هذه الدارسة بالأهمية الكبيرة على المستويين العملي والنظري. فهي تتناول من الناحية العملية مجموعة من النقاط الجوهرية في آن واحد، فمن جانب يتصل الأمر بتدهور القيم الاجتماعية في المجتمعات وشيوع ظاهرة الانحلال التي ما فتأت تنتشر حول العالم لتصل إلى مجتمعاتنا الشرقية، ومن جانب آخر تهدف الدراسة إلى توضيح الأركان القانونية لجرائم مستحدثة بدأت تشكل هاجس لعدد كبير من مستخدمي شبكة الإنترنيت ووسائل التواصل الاجتماعي، خاصة النساء، من قبيل التحرش الجنسي الإليكتروني والتنمر، في وقت سعي فيه المجتمع الدولي على مدار العقود إلى تكريس حقوق المرأة والدفاع عنها وخصص لها اتفاقية دولية خاصة وبرتوكولات ملحقه. أما على المستوي النظري فإن الباحثة تأمل في أن تمثل هذه الدراسة إثراءً للمكتبة القانونية، خاصة في البعد الخاص بالجرائم الإليكترونية والسيبرانيية.

إشكالية الدراسة:

تتمثل إشكالية الدراسة في أنها تتعلق بجرائم مُستحدثة، مما يتطلب البحث عن الدوافع الكامنة والأسباب الملموسة التي ساعدت على ظهورها، واستكشاف السبل المناسبة للتعامل معها. وفي ضوء توجه الدول العربية إلى اصدار قوانين خاصة بجرائم تكنولوجيا المعلومات، تحاول الدراسة توضيح الأهمية التي يجب أن تحظي بها هذه الجرائم التي تحظي حالياً باهتمام واضح ويتم بحثها في مؤتمرات دولية بهدف التوصل إلى توصيات مشتركة حول افضل طرق التعامل معها بما يحفظ الكرامة الإنسانية، ويحاسب المخالفين للقانون، ويتيح للإنسان حقه في استخدام تكنولوجيا المعلومات في أغراض وأهداف تساعد على تقدم ورقي الجنس البشرى، وليس الإضرار به واقحامه في مجال جديد من مجالات الجريمة يتسم بالغموض وتكثر فيه العقبات والتحديات.

وفضلاً عما تقدم، نشير إلى أنه من بين الإشكاليات التي تحاول الدراسة التعامل معها تحديد طبيعة الدوافع الكامنة وراء ظهور وتزايد جرائم التحرش الجنسي والتنمر الاليكتروني في العالم العربي كمجتمع شرقي له تقاليده وعاداته وهو الأمر الذي أصبح واقعاً ملموساً لا يمكن انكاره بل يلزم البحث عن توصيفه وطرح توصيات حتى سبل التعامل معه في إطار التعامل مع الجرائم الاليكترونية التي تعددت وتنوعت وفرضت نفسها على الإنسان المعاصر.

منهج الدراسة:

سوف تتبع الدراسة الحالية المنهج الوصفي التحليلي الذي يتعلق، من بين أشياء أخري، بوصف وتعريف الظاهرة محل الدراسة، مع الحرص على تحليليها من حيث معرفة أسبابها وتبعاتها على الأشخاص المعنية، خاصة وأن الأمر يتعلق بظاهرة متعددة الأبعاد، فهي ظاهرة نفسية اجتماعية، كما أنها تمثل جريمة قانونية تخضع لقانون العقوبات العادي أو قوانين تقنيات المعلومات عندما تتخذ الطابع الإلكتروني من خلال استخدام احدى وسائله كالهاتف النقال ومواقع التواصل الاجتماعي والبريد الإليكتروني وغيرها.

خطة الدارسة:

- **مقدمة.**
- **المبحث الأول: التحرش الجنسي الرقمي**
  - المطلب الأول: الماهية والأركان
    - الفرع الأول: التعريف.
    - الفرع الثاني: الأركان.
  - المطلب الثاني: التنمر الرقمي
    - الفرع الأول: التنمر من المنظورين التقليدي والإليكتروني
    - الفرع الثاني: أركان الجريمة
- **المبحث الثاني: الدوافع والتبعات**
  - المطلب الأول: الدوافع والانماط
    - الفرع الأول: التحرش الجنسي الإليكتروني
    - الفرع الثاني: التنمر الإليكتروني
  - المطلب الثاني: نظرة عامة على تبعات الجريمتين
- الخاتمة
- النتائج
- التوصيات
- قائمة المراجع

المبحث الأول: جريمة التحرش الجنسي الرقمي

المطلب الأول: الماهية والأركان

الفرع الأول: التعريف

تجدر الإشارة إلى أن الجريمة ذاتها أُطلق عليها العديد من المسميات ومن ذلك: التحرش عبر الانترنيت، التحرش الاليكتروني، التحرش عن بعد، التحرش الافتراضي، التحرش الرقمي، التحرش السيبراني، غير ذلك من المسميات التي تشير إلى استخدام شبكة الإنترنيت والعالم الافتراضي.

بصفة عامة يمكن القول إن التحرش الجنسي الرقمي ما هو إلا صورة مطورة أو معدلة من التحرش الجنسي الواقعي جاء كنتاج للتطور التكنولوجي مما جعل المتحرش- الذي يملك القدرة على استخدام شبكة الإنترنيت- إلى الانتقال من العالم الواقعي، بما قد يتضمنه من صعوبات أو عقبات أو مشاكل، إلى العالم الافتراضي الذي يتمتع فيه بحرية أكبر ومساحة أوسع للممارسة هذا الفعل المؤثم بشكل متكرر غير محدود دون خشية الرقابة أو المراجعة أو خوف من عقاب سواء أكان مجتمعي أو قانوني. ومن ثم فإنه لم تعد ظاهرة التحرش الجنسي قاصرة على الممارسات التي تتعرض لها الفتيات في الشوارع أو في الأعياد والمناسبات والزحام، وإنما أضحت تعدد النساء في منازلهن وأماكن عملهن من خلال شبكات التواصل الاجتماعي.

وفيما يخص التحرش الجنسي الواقعي فقد عرفته المادة (306) مكرر (أ) من قانون العقوبات المصري علي أنها "... كل تعرض للغير في مكان عام أو خاص أو مطروق بإتيان أمور أو ايحاءات أو تلميحات جنسية أو اباحية سواء بالإشارة أو بالقول او بالفعل بأية وسيلة بما في ذلك وسائل الاتصالات السلكية والسلكية.. إذا ارتكبت بقصد حصول الجاني من المجني عليه على منفعة ذات طبيع جنسية...".

وقد حرصت المادة على النص على تشديد العقوبة إذا كانت للجاني سلطة وظيفية أو أسرية أو دراسية على المجني عليه أو مارس عليه أي ضغط تسمح له الظروف بممارسته عليه أو ارتكبت الجريمة من شخصين فكثر أو كان أحدهم على الأقل يحمل سلاحاً...".

من هذا المنطلق، يُعرف البعض التحرش الجنسي الاليكتروني بأنه:

"استخدام شبكة الانترنيت في التواصل مع المرأة بقصد إيذائها والإضرار بها جنسياً وابتزازها مجتمعياً"، وبناء على ذلك تتم التفرقة بين التحرش في المجتمع الواقعي وذلك الاليكتروني، حيث أن الأول مادي والثاني رمزي لا يحدث فيه انتهاك مباشر للجسد. [544]

في المقابل، يعرفه البعض على أنه: استخدام للوسائل الاليكترونية والتواصل في توجيه الرسائل التي تحتوي على مواد تسبب الإزعاج للمتلقي لأهداف جنسية، أم كانت تحتوي على عبارات أو شتائم جنسية أو صور أو مشاهد فيديو جنسية أو التهديد والابتزاز باستخدام صور الضحية، أو استخدامها فعلاً من جون موافقة صاحبها أو من دون علمه، ومشاركتها عبر وسائل الاليكتروني المختلفة.[545]

وبالنظر إلى أن التحرش الجنسي عبر شبكة الإنترنيت ذو طبيعة خاصة تجعله يختلف عن ذلك الواقعي، فقد سعي الباحثون إلى تحديد أنماطه على النحو التالي:

1) **التحرش اللفظي**: والذي يتضمن ارسال كلمات خادشه للحياء أو التلفظ بكلمات ذات طبيعة جنسية في مكالمات صوتية أو وضع تعليقات تتضمن إيحاءات جنسية فجة.
2) **التحرش البصري**: ويتم من خلال ارسال صور أو مقاطع جنسية، أو حتى الطلب من الشخصية المستهدفة الكشف عن أجزاء من جسدها، وقد يصل الأمر إلى أن يقدم المتحرش على إرسال صور أو مقاطع فيديو له في أوضاع مخلة بالآداب يتفاخر بها.
3) **التحرش بالإكراه**: وفي هذه النمط يقوم المتحرش باختراق جـــهاز الاتصال الخاصة بالشخصية المستهدفة، والحصول على ما قد يتضمنه من صور خاصة أو معلومات شخصـــية، واستخدامها في الضغط عليها للقائه في العالم الواقعي إم عن طريق الابتزاز بنشر صور معينــة أو التشهير من خلال استخدام الوسائل الاليكترونية أو غير ذلك من الوسائل الفنية التي تتوقف على مدى تمكن المتحرش من استخدام تكنولوجيا المعلومات.[546]

---

[544] **محمود عبد العليم محمد سليمان، "التحرش الجنسي الإليكتروني: دراسة في الأنماط والدافع"، شبكة النبأ المعلوماتية، 2018/12/11، الرابط:**

https://annabaa.org/arabic/studies/13835

[545] **عمرو عبد العاطي، "التحرش الاليكتروني من الشارع إلى شبكات التواصل الاجتماعي"، 2015/4/28، الرابط:**

https://mustaqila.com

[546] **المرجع السابق.**

الفرع الثاني: الأركان

1) الركن المادي:

تتكون جريمة التحرش الاليكتروني، شانها في ذلك شأن باقي الجرائم، من ركن مادي يتمثل في نشاط إجرامي يقوم به الجاني، ونتيجة إجرامية، وعلاقة سببية تربط بين النشاط والنتيجة.

أ) **السلوك الإجرامي**: ويُقصد بذلك النشاط المادي الملموس الذي يقوم به الجاني أو يتقاعس فيه عن تنفيذ واجب قانوني مفروض عليه بما يوقعه تحت طائلة العقاب. وحيث هذا السلوك قد يكون إيجابي أو سلبي فإنه يلزم توضيح ذلك على النحو التالي:

- **السلوك الإيجابي**: وقد يتمثل في حركة إرادية يقوم بها الجاني لتنفيذ الجريمة المنسوبة إليه، وفي هذه الحالة قيام المتحرش بإرسال رسالة تحتوى على كلمات إباحية أو الفاظ جنسية على الصفحات الخاصة بصحيات التحرش الاليكتروني أو عبر البريد الاليكتروني الخاص بهم.[547]
- **السلوك السلبي**: ويُقصد به الإحجام أو التقاعس عن إتيان سلوك إيجابي محدد كان من الواجب اتخاذه حال توافر ظرف ما.[548] ومما لا شك فيه أنه في ظل التطور التقني الحالي يعتبر السلوك السلبي ركن له أهميته في جرائم التحرش الجنسي بوجه عام والتحرش الإليكتروني بوجه خاص، فالامتناع أو التقاعس المتمثل في الامتناع عن اتخاذ الاحتياطيات اللازمة يؤدى إلى وقوع حالات التحرش والتي قد تذهب إلى مدي أبعد من ذلك.

ب) النتيجة الإجرامية:

تتمثل النتيجة الإجرامية في حالة التحرش الإليكتروني في الأثر الذي يترتب على السلوك الإجرامي الذي يُحدد له القانون حماية جنائية.[549] وبطبيعة الحال تقوم التشريعات الجنائية بتحديد النتيجة الإجرامية بالنظر إلى طبيعة المصلحة المراد حمايتها بنصوص وخاصة بالتجريم والعقاب، ومن ثم فتوجد مصالح تحتاج إلى حماية لُمجرد تهديدها بالخطر، حتى ولو لم يترتب على ذلك آثار مادية، وهناك مصالح وحقوق لا يكفي لحمايتها مجرد التهديد بالخطر وإنما يلزم أن يترتب على ذلك آثار مادية محددة.[550]

[547] د. أحمد عوض بلال، مبادئ قانون العقوبات المصري: القسم العام، دار النهضة العربية، القاهرة، مصر، 1999، ص. 255.

[548] د. محمود نجيب حسن، قانون العقوبات: القسم العام، دار النهضة العربية، مصر، 1998 ص. 374-375.

[549] د. أحمد شوقي أبو خطوة، شرح الأحكام العامة لقانون العقوبات، دار النهضة العربية، مصر، القاهرة، 2000، ص 226.

[550] المرجع السابق، ص. 228.

ومما لا شك فيه أن عنصر النتيجة (بالمدلول المادي أو القانوني) يُعتبر من المسائل الشائكة التي يصعب اثباتها في جريمة التحرش الإليكتروني، ويعود ذلك إلى الطبيعة الخاصة لهذه الجريمة وما يترتب عليها من نتائج، فهناك نتائج قد لا تتحقق في الحال ولكن تحتاج إلى وقت، قد يطول أو يقصر، كما أنها قد تتحقق في مكان حدوث الفعل أو في مكان آخر. كما يلاحظ أن في جريمة التحرش الاليكتروني قد يتطلب المُشرع الجنائي حدوث نتيجة مادية معية تتمثل في الضرر الذي أدي إليه النشاط الإجرامي الذي ارتكبه الجاني، ليُقرر معاقبته، وأحياناً أخرى قد لا يتطلب المشرع تحقق نتيجة إجرامية معينة، وفي هذه الحالة ينصب التجريم على ذات النشاط الاجرامي للجاني بغض النظر عن أية نتائج مستقلة أخري يؤدى إليها. وإنه كانت السمة الغالبة في جرائم التحرش الاليكتروني هي ان يتطلب المشرع تحقق نتيجة معينة حتى يقرر اكتمال أركانها القانونية.

ج) النطاق الزماني والمكاني:

فيما يخص **النطاق الزماني**، تُعتبر غالبية جرائم التحرش الإليكتروني من الجرائم الوقتية لأن مناط ذلك هو السلوك الإجرامي ومدى استمرار وقت ارتكابه، فالنتيجة في جريمة التحرش الاليكتروني قد تتراخي للتحقق في زمان لاحق على ارتكاب النشاط الإجرامي. أما بالنسبة **للنطاق المكاني** فإن ما يميز جريمة التحرش الإليكتروني عن غيرها من الجرائم أنه قد يرتكب السلوك الإجرامي في مكان معين (الفضاء الافتراضي)، وتتحقق النتيجة الإجرامية في مكان آخر (العالم الواقعي).[551]

د) **علاقة السببية في جريمة التحرش الإليكتروني**

تكمن الأهمية القانونية للعلاقة السببية في أنها تربط ما بين عنصري الركن المادي (السلوك والنتيجة) فتقيم بذلك وحدته وكيانه وتجعل منه ظاهرة قانونية متماسكة العناصر والبنيان.[552] ووفقاً لما ذهب إليه المشرع المصري فإن جريمة التحرش الإليكتروني تُعد من الجرائم البسيطة حيث يكفي لقيامها ممارسة الأنشطة والوظائف المنصوص عليها قانوناً ولو لمرة واحدة لقيام الجريمة في حق مرتكبها ولا يتطلب لتمامها اعتياد ايتان الفعل وتكراره، وجاء ذلك على خلاف ما ذهب إليه المشرع الفرنسي. كذلك تُعتبر جريمة التحرش الجنسي الإليكتروني من الجرائم التي لا شروع فيها، بل تتم بمجرد القيام بقائمة أعمال تدخل في نطاق ما يرد من

---

[551] **د. محمود سيد أحمد عبد القادر عامر، إشكالية تحديد المسئولية الجنائية للتحرش الإليكتروني كجريمة اليكترونية والجهود الدولية لمكافحته، مجلة الدراسات القانونية والاجتماعية، جامعة مدينة لسادات، مصر، المجلد (7)، العدد (1) 2021، ص. 1-48.**

[552] **د. محمود نجيب حسنى، "علاقة السببية في قانون العقوبات"، طبعة نادي القضاة، مصر 1984، ص. 5.**

أنشطة، وفي المقابل فغنها لا تقوم بمجرد التحضير لهذه الأنشطة أو التمهيد لها أو محاولة الإتيان بها دون أن تقع بالفعل.[553] ومن ناحية أخرى تُعد هذه الجريمة من الجرائم الشكلية التي يكفي لقيامها مجرد القيام بالنشاط المادي المُجرم ،ولم يشترط المشرع المصري تحقيق نتائج معنية أو وقوع أضرار نتيجة لارتكاب هذا النشاط، وأخيراً، تُعد جريمة التحرش الإليكتروني من الجرائم الإيجابية والمستمرة.

2) الركن المعنوي

في تقديمة للركن المعنوي أوضح الأستاذ الدكتور محمود نجيب حسني أن هذا الركن يدور حول العلاقة التي تربط بين شخصية الجاني وماديات الجريمة، حيث يتمثل أساس هذا الركن في العلاقة النفسية التي تربط بين شخصية الجاني من جانب، وماديات ارتكاب الجريمة من جانب آخر. وأصل هذه العلاقة هو الإرادة، حيث لا يستطيع القانون تحديد المسئولية عن الجرم المحظور إلا بعد قيان علاقة بين ذلك الفعل وشخص من الأشخاص يُفترض توجه ارادته نحو ماديات الجريمة. وتتبلور إرادة الجاني في صورة القصد الجنائي وعلى أساسه: تكون الجريمة عمدية، أما الصورة الثانية فتكون الخطأ غير العمدي ومن ثم نكون بصدد جريمة غير عمدية.[554] وفي هذا السياق تجدر الإشارة إلى أن الكثير من جرائم التحرش الإليكتروني التي نصت المُشرع على تجريمها قد خلت من تحديد صورة الركن المعنوي الواجب توافره فيها؛ حيث توجد صعوبات عديدة تواجه اثبات هذا الركن، ومن ثم قد تعجز النيابة العامة عن اثبات توافر القصد الجنائي أم تعلق الأمر بخطأ.

المطلب الثاني: التنمر الرقمي

الفرع الأول: التنمر من المنظورين التقليدي والإليكتروني

يُرجع الكثير من الباحثين ظهور مفهوم التنمر إلى طلاب المدارس، الأمر الذي جعل معظمهم يربط بينه وبين البيئة المدرسية، باعتبارها أكثر الأماكن صلاحية لظهور ونشأة هذا السلوك وممارسته. ومع تزايد استخدام طلاب المدارس والشباب لوسائل التكنولوجيا الحديثة وتطبيقات الإنترنيت، تم استنساخ ظاهرة التنمر ونقلها إلى الفضاء الإليكتروني فيما يُطلق عليه التنمر الاليكتروني.

يُقصد بالتنمر بمعناه العام حالة من السلوكيات السلبية المتكررة القصد منها الإيذاء أو المضايقة، تصدر من شخص قوي ضد شخص أقل قوة. كذلك يتم تقديمه على أنه: أفعال سالبة من جانب تلميذ أو أكثر تُلحق

---

[553] المرجع السابق.

[554] المرجع السابق، ص. 524-525.

الأذى بتلميذ آخر، تتم بصورة متكررة وطوال القت، ويكن أن تكون هذه الأفعال السالبة بالكلمات (مثل التهديد، التوبيخ، الإغاظة، الشتائم) كما يمكن أن تكون بالاحتكاك الجسدي (كالتكشير بالوجه، أو القيام بإشارات غير لائقة) بقصد عزله من المجموعة أو رفض الاستجابة لرغبته.

وأيضاً تم تعريف التنمر على أنه: شكل من أشكال العدوان، لا يوجد فيه توازن للقوي بين المتنمر والضحية ودائماً ما يكون الأول أقوي من الثاني.[555]

يتسم التنمر التقليدي، بشكل عام، بثلاث سمات رئيسية:

1) فعل عدواني بواسطة شخص ما (المتنمر) موجه ضد شخص آخر (الضحية)، بهدف إيقاع الضرر بالأخير.
2) التفاوت في القوة بين المتنمر والضحية، بما يعنيه ذلك من عدم قدرة الأخيرة على الدفاع عن نفسها بسهولة. وقد يتعلق هذا التفاوت بالقوة الجسدية، أو العمر الزمنى، أو الحالة المادية، أو المستوي الاجتماعي.
3) تكرار الفعل عبر الوقت والسياقات.

وفي واقع الأمر تم تصنيف التنمر التقليدي إلى أربعة أنماط رئيسية:

1) **التنمر الانفعالي**: حيث يسعي المُتنمر إلى التقليل من شأن الضحية من خلال التجاهل، العزلة، السخرية، الاحتقار المتكرر، أو ردود الأفعال العدوانية تجاه الضحية.
2) **التنمر البدني**: بمعنى إلحاق الأذى بالضحية بطرق مختلفة، وفقاً للجنس فمن التصرفات الشائعة بين الذكور: الدفع، الضرب، الركل، افساد ممتلكات الضحية، أما فيما بين الإناث فإنهن يستخدمن التلسين، وإثارة الفتن والشائعات حول الضحية.
3) **التنمر الاجتماعي**: ويُقصد بذلك خلق حالة من العزلة حول الضحية وانتقاد تصرفاتها الاجتماعية بصفة مستمرة، ورفض صداقتها أو مشاركتها في أي شيء وتجاهلها بشكل متعمد.

---

[555] د. ثناء هاشم محمد، "واقع ظاهرة التنمر الإليكتروني لدي طلاب المرحلة الثانوية في محافظة الفيوم وسبل مواجهتها: دراسة ميدانية"، مجلة جامعة الفيوم للعلوم والتربية النفسية، العدد الثاني عشر، الجزء الثاني، مصر، 2019، ص. 180 وما بعدها.

4) **التنمر اللفظي**: ويتسم هذه النمط بقيام المتنمر بتهديد الضحية أمام مجموعة من الأقران بقصد السخرية والاستهزاء والتشهير، كما تهدف الالفاظ والكلمات المستخدمة إلى الحاق الأذى النفسي بالضحية ومضايقتها بصورة متكررة.

وفي هذا السياق، يأتي **التنمر الإليكتروني** ليمثل أحدث وسائل التنمر، حيث أنه يستخدم الوسائل والتقنيات الحديثة كالإنترنيت والهاتف المحمل، لإرسال الرسائل غير المرغوبة، أو نشر الشائعات... وبعبارة أخرى لإلحاق الضرر المتعمد والمتكرر الذي يستهدف فرد معين أو مجموعة من الأفراد.[556] فيُعد التنمر الإليكترون انتهاك للحياة الخاصة للآخرين عن طريق المطاردة الإليكترونية والتي هي امتداد للمطاردة الجسدية أو ما يُسمي التنمر التقليدي.

ومن جانبها، تُعرف منظمة الأمم المتحدة للطفولة (اليونيسف) التنمر الإليكتروني بأنه: التنمر باستخدام التقنيات الرقمية، ويمكن أن يحدث على وسائل التواصل الاجتماعي ومنصات المراسلة والألعاب والهواتف المحمولة، وهو سلوك متكرر يهدف إلى إخافة أو استفزاز المستهدفين به أو تشويه سمعتهم. ومن أمثلة ذلك:

- نشر الأكاذيب عن شخص ما أو نشر صور محرجه له على وسائل التواصل الاجتماعي.
- إرسال رسائل أو تهديدات مؤدية عبر منصات المراسلة.
- انتحال شخصية شخص ما وإرسال رسائل جارحة للآخرين.[557]

وتجدر الإشارة إلى أن التنمر الإليكتروني يُعد أكثر خطورة من ذلك التقليدي لمجموعة من الأسباب أبرزها ما يلي:

- يعتمد على درجة معينة من الخبرة التكنولوجية تمكن المُتنمر من إرسال رسائله الإليكترونية أو النصية، ثم التخفي لنفي الهجمات عن نفسه والادعاء بقيام شخص آخر بتشوية سمعة الضحية.
- عدم قدرة الضحية على الاختباء لصعوبة الهروب من التنمر الإليكتروني الذي يتابعها أينما كانت من خلال الرسائل المرسلة عبر الهاتف أو الكمبيوتر أو التعليقات المسيئة عبر مواقع الإنترنيت.

---

[556] **المرجع السابق.**

[557] **كلير ماكفيير، "التنمر الإليكتروني: ما هو وكيف يمكن إيقافه"، موقع منظمة الأمم المتحدة للطفل، اليونيسيف، 11 فبراير 2020، الرابط:**

https://www.unicef.org/jordan/ar

- إمكانية وصول المتنمر الإليكتروني إلى جمهور أكبر (من خلال الإنترنيت) مما هو موجود في المجال المدرسي.
- تمتع المتنمر من مضايقة الضحية في أي وقت، مع التقليل من فرص محاسبته على فعلته عما هو في التنمر التقليدي نظراً لإمكانية التخفي في غياهب شبكة الإنترنيت.
- عدم المواجهة المباشرة، كما هو في حالات التنمر التقليدي، نتيجة لعدم وجود الطرفين وجهاً لوجه، الأمر الذي يتيح فرصة أكبر للمتنمر لعدم الكشف عن هويته والتقليل من المخاطر التي قد يتعرض لها إذا مت تم التعرف عليه من قبل الضحية.
- كثرة انتشاره في حياة الضحية، فهو لا يتقيد بالتواجد في مكان بعينه معها (مبنى المدرسة) بل يستطيع يصل إليها في أي مكان من خلال الهاتف النقال أو البريد الاليكتروني أو أي من وسائل التواصل الاجتماعي.

الفرع الثاني: أركان الجريمة

تتكون جريمة التنمر الاليكتروني، شانها في ذلك شأن التحرش الجنسي الإليكتروني، من ركن مادي يتمثل في نشاط إجرامي يقوم به الجاني، ونتيجة إجرامية، وعلاقة سببية تربط بين النشاط والنتيجة.

1) الركن المادي:

كما سبق ايضاحه، يمُثل الركن المادي للجريمة وجهها الذ يبدو في الخارج متمثلاً في الواقعة المادية التي صدرت من مرتكبها معبرة عن إرادته الآثمة، فلا يعتد القانون بمجرد التفكر او النوايا، أو مجرد المعتقدات التي لا تتجسد في عمل خارجي. ويتمثل مضمون الركن المادي في ثلاثة عناصر هي: السلوك الإجرامي، والنتيجة، وعلاقة السببية.[558]

- **النشاط الإجرامي الإيجابي**: ويتخذ شكل قيام الجاني المنسوب إليه الجريمة، وفي هذه الحالة قيام المُتنمر بإرسال رسالة أو مشاركة مقاطع فيديو لشخص بصور تجعله عرضة للاستخفاف والإهانة والإحراج. وقد يكون من شأن ذلك العمل على اغتيال الشخصية من خلال ارسال معلومات مزيفة وغير صحيحة، واختلاف الأكاذيب والافتراءات التي تهدف على تسوية الحقائق

---

[558] **د. أحمد فتحي سرور، الوسيط في قانون العقوبات: القسم العام (قانون العقوبات ونطاق تطبيقه- التجريم والإباحة- الجريمة- المجرم- العقوبة) مطورة ومحدثة، دار الأهرام للنشر التوزيع والإصدارات القانونية، الطبعة السادسة، القاهرة، مصر، 2014، ص. 527 وما بعدها.**

والسخرية ونشر الشائعات حوله. كذلك قد يتمثل النشاط الإجرامي في انتحال الهوية من خلال اختراق حساب شخصي لشخص ما وانتحال شخصيته لإرسال معلومات وأمور محرجة عن الآخرين.[559]

- **النتيجة الإجرامية:** يُعد التنمر الإليكتروني انتهاكاً للحياة الخاصة للآخرين عن طريق المطاردة الإليكترونية وتتعدد النتائج التي قد تترتب على هذا السلوك وتتنوع في الاستجابات العاطفية كالخوف الدائم والإحباط، والغضب، والاكتئاب، والعزلة عن الناس والمجتمع، وقد ينتهي المطاف إلى الانتحار.[560]

- **علاقة السببية:** من المسلم به أن السلوك الإجرامي في الجريمة التامة لا ينفصل عن النتيجة المادية، فكلاهما فكرتان متلازمتان لا غنى لإحداهما عن الأخرى، ولا تقوم الجريمة إلا إذا كانت النتيجة بناء على السلوك الإجرامي، ويُحقق هذا التلازم القانوني بين السلوك الإجرامي والنتيجة رباطاً مادياً بينهما لقيام الركن المادي. ومن حيث إثبات الجريم إلى شخص معين يجب أن يثبت أن مساهمته الجنائية هي التي أدت إلى النتيجة المادية.[561]

وفي هذا الخصوص تجدر الإشارة إلى أن جريمة التنمر الإليكتروني شأنها شأن تلك الخاصة بالتحرش الجنسي الإليكتروني تخضع لنفس القواعد في القانون المصري، من حيث اتصافها بالشكلية.

- **الركن المعنوي:** كما سبق ايضاحه فإنه لا يكفي لوقوع الجريم توافر مادياتها الظاهرة والواضحة أمام العيان، وإنما يجب بالإضافة إلى ذلك أن تتعاصر مع هذه الماديات إرادة إجرامية تبعث هذه الماديات إلى الوجود، ويُعبر عن هذه الإرادة الإجرامية بالركن المعنوي. ويفترض الركن المعنوي بوصفه اتجاهاً إرادياً آثماً، أن يكون معاصراً للركن المادي متمثلاً في السلوك الإجرامي الذي

---

[559] روعة نضال الشقران، التنمر الإليكتروني وآثاره القانونية والاجتماعية، وكالة أنباء عمون، الأردن، 15 أكتوبر 2020، الرابط: https://www.ammonnews.net/article/568376

[560] المرجع السابق.

[561] د. أحمد فتحي سرور، مرجع سابق، ص. 615.

أفضي إلى النتيجة. فإذا توافر في لحظة لاحقة على السلوك الإجرامي، فإنه لا يكون كافياً لوقوع الجريمة.[562]

وكما الحال بالنسبة للتحرش الجنسي الإليكتروني فإنه الكثير من جرائم التنمر الإليكتروني التي نص المشرع على تجريمها قد خلت من تحديد صورة الركن المعنوي الواجـــب توافره فيها، وإن كان في كافة الأحوال تتوافر النية والإرادة في احداث الضرر بالضحية على النحو السابق إيضاحه.

المبحث الثاني: الدوافع والتبعات

المطلب الأول: الدوافع والأنماط

الفرع الأول: التحرش الجنسي الإليكتروني

يتنوع ويتزايد عدد الذين يقدمون على ارتكاب جريمة التحرش الجنسي الإليكتروني[563] من حيث الدوافع والطبيعة الشخصية، وقد قام البعض بتصنيفهم إلى ثلاثة أنماط:

النمط الأول: اشخاصاً يخشون مواجهة الآخر، فيتحرشون بأشخاص لا يعرفونهم للبعد عما يخشونه، وينتشر هذا النمط بين الشخصيات المنغلقة المحرومة من الحريات، حيث يجد المتحرش في هذا النمط في الأحاديث عبر الإنترنيت متنفساً له، بل المتنفس الوحيد.

النمط الثاني: ويضم الأشخاص الذين يشعرون بالسعادة لقيامهم النصب على الآخرين أو استغفالهم أو مضايقتهم، وبطبيعة الحال فإن الأمر يتعلق في هذا النمط بشخصيات غير سوية لها دوافعها المتصلة بطبيعة تركيبها النفسي.

---

[562] المرجع السابق، ص 643.

[563] في هذا السياق نشير إلى النتيجة التي توصل إلى تم اعدادها بناء على طلب من صحيفة الوطن السعودية على عينة من الجنسين من مختف المناطق من فئة الشباب من عمر 13 إلى 26، بهدف استقصاء ظاهرة التحرش الإليكتروني في السنوات الأخيرة، فقد أوضحت ارتفاع نسبة التحرش الإليكتروني في المملكة العربية السعودية 70%، فضلاً عن أنه يبدأ من عمر 11 عاماً، ويتركز في الفئة العمرية محل الدراسة، ومن المفارقات أن الدراسة أشارت إلى ارتفاع هذه الظاهرة بين الفتيات عبر مواقع التواصل الاجتماعي، مستغلات في ذلك الأسماء المستعارة. الرابط:

عالية الشريف، "ارتفاع التحرش الإليكتروني عند الشباب بنسبة 70%"، جريدة الوطن السعودية، 25 مارس 2016، الرابط:

https://www.alwatan.com.sa/article/295316

النمط الثالث: ويشمل أولئك الذي يشعرون بسعادة جنسية بالغة وإثارة لمجرد نطقهم كلمات تتضمن إيحاءات جنسية خلال محادثاتهم على شبكة الإنترنيت، ومن المفارقات هذه السعادة قد تزداد عندما تقابل أحاديثهم بالرفض أو الإهانة، مما يدفعهم إلى معاودة الكرة.[564]

يتناول هذا البحث جريمتين يتم ارتكابهما في الفضاء الإليكتروني تتصلان، بشكل رئيسي، بالنساء والفتيات كضحايا سواء تعلق الأمر بالتحرش الجنسي الإليكتروني أو التنمر، وإن كانت هناك حالات تمس الشباب من الذكور بدرجة أقل. وفيما يتعلق بالتحرش الجنسي على وجه الخصوص، تلزم الإشارة إلى ما يمكن تسميته بإشكاليات الفهم الذكوري لسيكولوجيا الرغبة الجنسية لدي الأنثى، والتي يمكن تلخيصها في الأفكار الخاطئة السائدة في هذا الخصوص وأبرزها:

1) الأنثى كائن متردد لا يعي حاجته ورغبته، كما أن المقولة التي يلزم تطبيقها على إطلاقها هي تلك القائلة "تتمنعن وهن راغبات".
2) الأنثى طالبة للتحرش: وتنطوي هذه الفكرة على خلط كبير بين الرغبة البشرية في الاستماع إلى الإطراء الجسدي والروحي بما يُشبع الحاجة للشعر بالثقة والتميز، وهو ما ينطبق ليس فقط على الإناث ولكن أيضاً على الذكور.
3) الأنثى راغبة في الاغتصاب دون تصريح، وهو على العكس تماماً مما يشاهده الذكور في مقاطع التحرش والاغتصاب الإباحية التي ما هي إلا مجرد مقاطع تم تصويرها لأغراض معينة ولا علاقة لها بالواقع أو الحقائق النفسية لطرفي العلاقة.
4) الأنثى البعيدة عن الممارسة الجنسية مختلة نفسياً أو متلهفة لهذه الممارسة.[565]

---

[564] **محمود عبد العظيم محمد سليمان، "التحرش الجنسي الإليكتروني: دراسة في الأنماط والدوافع"، شبكة النبأ المعلوماتية، 11 ديسمبر 2018، الرابط:**

https://annabaa.org/arabic/studies/13835

[565] **تامر البطراوي، "ظاهرة التحرش: تحليل سيكولوجي سوسيولوجي، موقع شبكة الحوار المتمدن، 16 مارس 2018، الرابط:**
https://www.ahewar.org/debat/show.art.asp?aid=592462

وفضلاً عما تقدم فإن ظاهرة التحرش الجنسي (في العالم الواقعي أو الافتراضي) ليس لها نموذج واحد، حيث يقوم بها أطراف كثيرون كالمتزوج، والمدير، والزميل، والجار، والفقير، والغنى، والطفل الصغير، والشاب، وكبير السن، كما أنها تمتد لتشمل الدول النامية والمتقدمة على حد سواء.[566]

وفي ضوء ما تقدم، فإنه يلزم الإشارة إلى الدوافع وراء هذه الظاهرة التي لا ترتبط بالسن أو الوضع الاجتماعي أو درجة التقدم والتحضر، ومن بين هذه الأسباب نشير إلى ما يلي:

أولاً- التراجع الذي أصاب منظومة القيم الاجتماعية في المجتمع العربي، وما تبعه من بروز منظومة قيمية جديدة كانت نتاج للتغير الاجتماعي السريع في المجتمع، ومن أبرز ملامحها تراجع المعني السليم للتدين، وانفصال السلوك الواقعي عن السلوك الديني.

ثانياً- النظر إلى المرأة باعتبارها جسدًا: ويُقصد بذلك أن المنظومة القيمية الجديدة اختزلت المرأة في مجرد كونها جسد فاتن، في حين توارت صورة المرأة ككائن اجتماعي واع يسهم، كما هو الحال بالنسبة للرجل، في نهضة الأمة وتطورها.

ثالثاً- عدم نجاعة أساليب التربية والرقابة الأسرية: فقد أثبتت كثير من الدراسات تقصل دور الرقابة الأسرية، ونقص القدرة على الوعي والتوجيه، فضلاً عن عدم توفير الإشباع العاطفي للأبناء وحتى البالغين منهم. ويضاف إلى ذلك عدم اتباع أساليب الحوار الجاد وإنما التربية بالمنع والعقاب عوضاً عن التوعية والإشباع النفسي.

رابعاً- القناع الرقمي أو سهولة إخفاء الهوية: ويترتب على ذلك المساهمة في المزيد من المتحرشين الذين تمكنهم هذه الصفة من التغلب على ما قد يعانون من خجل، ليتحولوا إلى ذئاب بعيداً عن رقابة المجتمع لتصرفاتهم التي قد تسفر في الواقع العملي عن نظرة سلبية وعزلة في المجتمع.

خامساً- الرغبة في الانتقام من عدم القدرة على المواجهة: في هذا الخصوص تذهب بعض الدراسات إلى أن من يلجئون إلى التحرش الإليكتروني، باعتباره وسيلة لإزعاج ضحاياهم، يعانون من تقدير متدن للذات، كما أن لديهم اضطراب في الشخصية يقلل من قدرتهم على تقدير نتائج أفعالهم، ومن ثم فإنهم يقدمون على مثل هذه الأفعال التي تجعلهم في منأى عن العقاب، كوسيلة لتعويض الضعف والانتقام والشعور بالقوة والسيطرة.

---

[566] **المرجع السابق.**

سادساً- الحرمان الجنسي: ويمثل هذا انعكاساً لتأخر سن الزواج مما يسهم في تزايد الشعور بالحرمان، ويؤدى إلى سعي الشباب إلى التخلص من هذا الشعور من خلال التحرش الإليكتروني الذي قد يؤدي في بعض الحالات إلى الإشباع الجسدي الحقيقي لهذه الرغبات.

سابعاً- الانفتاح الاجتماعي الناتج عن سهولة الاتصال الإليكتروني: وقد ترتب على ذلك صدمة ثقافية عانى البعض، في ظلها، من عصوبة في إدارة علاقاته مع الآخرين بشكل صحيح وفي إطار علاقات الصداقة المجردة.

ثامناً- الترويج المستمر عبر وسائل الإعلام للعلاقات الجنسية بالمفهوم الغربي من خلال ترجمة وعرض الأفلام والمسلسلات الأجنبية التي تختصر العلاقة بين الرجل والمرأة في الاتصال الجنسي بشكل مباشر دون القيام بتقنين هذه العلاقة بشكل مسبق.

الفرع الثاني: التنمر الإليكتروني

أصدرت الهيئة الوطنية لتنظيم الاتصالات في مملكة البحرين بالتعاون مع برنامج "كن حراً" التابع للجمعية البحرين النسائية للتنمية الإنسانية كتيباً حول التنمر الاليكتروني[567] رصد نمطين رئيسيين له هما:

- **التنمر المباشر**: ويُقصد به أن يقوم المُتنمر بإرسال ما يؤذى الضحية بشكل مباشر.
- **التنمر غير المباشر**: ويكون في الحالة التي يُرسل فيها المتنمر ما يؤدى إلى إيذاء الضحية أو الآخرين في موقع يشترك فيه آخرون، مما يجعل من هذه النمط الأكثر خطورة نظراً لما يترتب عليه من انشار على نطاق واسع، وعادة ما تكون تبعاته متشعبة وغير قابلة للسيطرة عليها.

تشير الدراسات والأبحاث إلى أن أهم أسباب التنمر الإليكتروني تتمحور حول ما يلي:

- **العامل النفسي**: وهو الذي يدفع الفرد إلى التنمر؛ لغرض تأكيد ذاته من خلال استهزائه واعتدائه على الآخرين. ففي واقع الأمر، شأنه شأن بعض المتحرشين جنسياً عبر الإنترنيت، المتنمر هو إنسان ضعيف لا يستطيع المواجهة، ويعتقد أنه بتخفيه خلف القناع الإليكتروني سيشعر بالقوة والسيطرة والتملك.

---

[567] **"قل لا ... للتنمر الإليكتروني: أحمي نفسك من التنمر الإلكتروني... وساهم في حماية الآخرين". كتيب صادر عن هيئة تنظيم الاتصالات، جمعية البحرين النسائية، مملكة البحرين، بدون تاريخ، الرابط:**

https://bahrainws.org/

- **العامل الأسري**: ويُقصد بذلك طبيعة العلاقات الاجتماعية داخل الأسرة، فعندما يلاحظ الطفل أن الأب يستعمل أسلوب القوة والعقاب والتنمر وغيرها من الأساليب السلبية، فإن من شأن ذلك أن يسعي الطفل إلى اتباع نفس الأساليب حتى يشبع رغبته في الشعور بالقوة.[568]

- **أسباب ذاتية**: يسعي المتنمر إلى تغطية ضعفه وعدم قدرته على تغيير شخصيته وحياته بوضعها القائم، ومن ثم فإنه يقنع نفسه بأن في استطاعته أن يغير من حياة الآخرين والتأثير على وضعهم وحالهم حين يشاء. فعلي سبيل المثال يري أنه يمكنه أن يجعل شخصاً ما يحزن أو يغضب أو يتأثر بشكل سلبي، وكلها مشاعر وأحول يمر بها المتنمر ذاته ويشعر بها، ولا يعرف كيف يتعامل معها ومن ثم يريد أن ينقلها إلى الآخرين.

- **أسباب تتعلق بالآخرين**: قد يهدف المتنمر بسلوكه إلى نشر الشعور لدي الآخرين بأن لديه قوة وشجاعة وأن عليهم أن يخافوا منه ويحسبون له حساباً، فهو شخص قادر على الإيذاء، وبالتالي يلزم عليهم الحصول على رضاه كي لا يقدم على إيذائهم.[569]

- **أسباب تتعلق بطبيعة شبكة الإنترنيت**: ومن ذلك قدرته على الإفلات من العقاب نتيجة لضعف القوانين المتصلة بذلك، وربما لعدم وجود أدلة كافية، أو توافر إمكانية استخدام حسابات مزيفة مما يصعب من عملية التوصل إلى الفاعل.

- **أسباب تتعلق بمرحلة المراهقة** ومن بين هذه الأسباب نشير إلى ما يلي:

1) يوفر التنمر الإليكتروني مساحة واسعة للمراهق لإشباع رغبته في التجربة وما يتميز به في سنه من حب للإثارة.
2) يحاول المراهق أن يثبت لنفسه أنه قد تخطي مرحلة الطفولة وأن أفضل السبل إلى ذلك هو القيام بكل ما من شأنه المساهمة في ترسيخ شعور السيطرة لديه، ومن ذلك القدرة على السيطرة على مشاعر الآخرين وإدخال الخوف والرعب إلى قلوبهم.

---

[568] محمد حسون، "التنمر الإليكتروني بين الأسباب والعلاج، موقع العطاء الرقمي، الرابط:
https://attaa.sa/library/view/385

[569] "قل لا ... للتنمر الإليكتروني: أحمي نفسك من التنمر الإلكتروني... وساهم في حماية الآخرين"، مرجع سابق ذكره.

3) ميل المراهق إلى جذب الانتباه لنفسه، وأن يكون مصدراً للإثارة، وهو الأمر الذي قد يتصور إمكانية تحقيقه من خلال ممارسة التنمر الإليكتروني.[570]

المطلب الثاني: نظرة عامة على تبعات التحرش الجنسي والتنمر الإليكتروني

مما لا شك فيه أن كل من التحرش الجنسي والتنمر الإليكتروني يترتب عليه تبعات سلبية على الضحية أو الشخص المستهدف، فبالنسبة للتحرش الجنسي ينتهي الأمر بالعديد ممن يتعرضن هل إلى الانعزال عن محيطهم والهور من المجتمع، كذلك فإنه هناك مضاعفات نفسية كثيرة يعانون منها لفترات طويلة تمتد لسنوات.

في هذا الخصوص أوضحت إحدى الدراسات الحديثة في دورية طبية أمريكية[571] أن هؤلاء الضحايا يصبحن أكثر عرضة من غيرهن للإصابة بالقلق والاكتئاب والرهاب والقلق.

أما بالنسبة للتنمر الإليكتروني فإن هناك العديد من الآثار المدمرة من قبيل:

- صعوبة الثقة بالآخرين والنظر إليهم بعين الشك.
- ضعف الثقة بالنفس والنظرة الدونية للذات.
- تشتت الذهن وتدني المستوى الدراسي.
- الخوف والقلق والترقب.
- التعرض لأمراض نفسية وجسدية.
- المعاناة من اضطرابات في النوم وتناول الطعام.
- عدم الرغبة في الذهاب إلى المدرسة أو التواجد في أماكن التجمع.[572]

الخاتمة

فتح التطور الهائل التي شهدته تكنولوجيا المعلومات آفاقاً واسعة أمام الإنسان لتحقيق العديد من الأهداف التي كان من الصعب تصور إمكانية تحقيقها، فعلي سبيل المثال لم يعد الباحث في حاجة إلى التنقل بين المكتبات الجامعية بحثاً عن مراجع حول موضوع معين، بل أصبح في مقدورة عمل اشتراك يسمح له بالدخول

---

[570] المرجع السابق.

[571] محمود عبد العظيم محمد سليمان، مرجع سابق ذكره.

[572] "قل لا ... للتنمر الإليكتروني: أحمي نفسك من التنمر الإلكتروني... وساهم في حماية الآخرين"، مرجع سابق ذكره.

إلى هذه المكتبات أو أغلبها والحصول على ما يريد من معلومات بسهولة وسرعة. كذلك أصبح من السهل نقل المعلومات مباشرة من كافة بقاع العالم وقت حدوثها، بل وساعدت في كثير من الأحيان على التعرف على الجناة في العديد من الجرائم. وفي المقابل تم رصد تحرك موازي من قبل الأفراد والمجموعات ومنظمات الجريمة إلى الاستفادة بدورها من هذا التطور لتحقيق أغراضها الإجرامية، فهناك من الأفراد من سخرها لممارسة التحرش الجنسي الإليكتروني، وهناك من استخدمها للتنمر الإليكتروني، إلى غير ذلك مما أصبح يُطلق عليه الجرائم الإليكترونية.

وهكذا، فإنه في عصر السماوات المفتوحة لم تعد ظاهرة التحرش الجنسي أو التنمر قاصرة على الممارسات في العالم الواقعي، ولكن أصبح من الممكن ممارستها في العالم الافتراضي وبشكل مستمر وفي أي وقت أو مكان من خلال استخدام وسائل التواصل الاجتماعي المرتبطة بشبكة الإنترنيت، وفي ظل تنامي وتزايد عدد هذه الحالات التي يتخفى فيها الجاني في الفضاء الافتراضي، بات من الضروري وضع آليات للتعامل معها.

موقف بعض القوانين (القانون المصري) النتائج والتوصيات

النتائج:

تلقي الدراسة الضوء على الأركان الواجب توافرها قانوناً في جرائم الإنترنيت والتي وان تماثلت مع تلك الخاصة بالجرائم الواقعية فإنها تتسم بطابع خاص، وفي هذا الصدد نشير إلى ما يلي:

- يتطلب الركن المادي في جرائم الإنترنيت وجود بيئة رقمية واتصال بالإنترنيت، وكذلك معرفة بداية هذا النشاط والشروع فيه ونتيجته. ويُلاحظ في هذا الخصوص أنه ليس كل جريمة اليكترونية تستلزم وجود أعمال تحضيرية، بل أن يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي. وإذا كان القانون الجنائي لا يعاقب على الأعمال التحضيرية في الجرائم الواقعية إلا أن الأمر يختلف فيما يتعلق بتكنولوجيا المعلومات، فعلي سبيل المثال شراء معدا لفك الشفرات ولكمات المرور وبرامج اختراق، وحيازة صورة دعارة للأطفال تمثل جرائم في حد ذاتها.[573]

[573] **اللواء د. فؤاد جمال، الجرائم المعلوماتية، دار النشر الحديثة، مصر، 2011، ص 12-13.**

- صعوبة تحديد الركن المعنوي، والمتمثل في الحالة النفسية للجاني والعلاقة التي تربط بين شخصيته وماديات الجريمة، في الجرائم الاليكترونية، فقد تنقل المُشرع في تحديد هذا الركن بين مبدأ الإرادة ومبدأ العلم، أما بالنسبة للقضاء الفرنسي فإنه يسود منطق سوء النية؛ حيث يشترط المشرع وجود سوء نية في الاعتداء على بريد إليكتروني خاص بأحد الأشخاص.[574]

- في بعض الأحيان توجد صعوبة في مواجهة هذه الأنواع من الجرائم المُستحدثة، ترجع إلى أن العيد من الحسابات التي يتم استخدامها لذلك هي في حقيق الأمر حسابات مُزيفة يتم أقفالها بعد فترة من استخدامها من قبل مرتكب مثل هذه الجرائم، ليقوم بفتح حسابات أخري يستخدمها لنفس الغاية أيضاً لفترة محدودة، الأمر الذي يشكل عقبة فنية أمام كشف حقيقته والوصول إليه لمقاضاته.

- ارتبط انتشار جريمتي التحرش الجنسي والتنمر الإليكتروني بعصر أصبح من المعتاد فيه استخدام شبكة الإنترنيت ووسائل التواصل الاجتماعي بشكل يومي مستمر، والدخول في العديد من العلاقات الافتراضية، غير أن البعض عمد إلى تسخير الإمكانيات التكنولوجية الحديثة لتحقيق غير أخلاقية وإشباع غرائز غير سوية مما فتح الباب أمام الحديث عن جرائم الإنترنيت بشكل عام والتحرش الجنسي والتنمر الإليكتروني بشكل خاص.

- يتطلب الأمر اصدار قوانين تتضمن عقوبات رادعة يتم تطبيقها على الجناة لحماية الضحايا من التبعات السلبية من جانب، والقضاء على الظواهر الاجتماعية السيئة التي تسيء إلى المرأة أو الفتاة بصفة خاصة، والمجتمع بصفة عامة، خاصة عندما نتحدث عن مجتمع شرقي عريق له عاداته وتقاليده المستمدة من حضارات قديمة وأديان سماوية تحض على مكارم الأخلاق وتحرم ارتكاب الافعال المشينة بكافة أنواعها وصورها.

- لم تعد احتمالية تعرض الشخص- خاصة النساء والفتيات- للتحرش الجنسي أو التنمر مقتصرة فقط على لقاء مباشر في الطريق العام بين مرتكب الجريمة والضحية الممارس في حقها الفعل، بل أصبح من اليسير الوصول إلى الضحية بطريقة ليست فقط تتميز بالسهولة وإنما تصبغ على الجاني صفة السرية حيث يمكنه تقديم نفسه باسم مختلف وببريد اليكتروني تم خلقه خصيصاً لاستخدامه في هذه

---

[574] المرجع السابق.

الأغراض، مما يبعد الشبهات عن الجاني ويُصعب من عملية الوصول إليه استناداً إلى المعلومات الواردة عن مستخدم الحساب.

التوصيات:

- أهمية التوصل إلى اتفاق شامل على المستوي العربي لمكافحة جرائم تكنولوجيا المعلومات، يتضمن النص الصريح على جريمتي التحرش الجنسي والتنمر الإليكتروني ويضع تعريفاً متفق عليه لكلتا الجريمتين، وأسس للتعاون بين الدول في تبادل المعلومات حول مصدر الرسائل المتضمنة أركان الجريمة في كلتا الحالتين، خاصة مع ما توفره الشبكة العنكبوتية من إمكانية ارسال الرسائل من شخص يقيم في دولة أخري إلى ضحيته، وقيامه في مرحلة أخري بنقل تفاصيل ذلك إلى شخص ثالث يقيم في الدولة التي تتواجد فيه الضحية ليستكمل العلاقة في حالة تطورها.
- التأكيد على الدور الوقائي الذي يلزم أن تعلبه الأسرة لمواجهة مثل هذه الجرائم وذلك من خلال توعية الفتات بالمخاطر التي تحتويها شبكة الإنترنيت، ومواقع التواصل الاجتماعي، فضلاً عن تقديم النصائح المتصلة بالطرق الآمنة لاستخدام الشبكة العنكبوتية من حيث عدم عرض بيانات شخصية، وعدم قبول طلبات صداقة من أشخاص غير معلومين بشكل شخصي، واستخدام كافة أدوات الأمان التي توفرها المواقع الإليكترونية لحماية المعلومات الشخصية.
- ضرورة قيام جمعيات المجتمع المدني بدور في نشر التوعية بخطورة هذه الجرائم وتبعاتها، وذلك من خلال خلق قنوات اتصال مع النساء والفتيات وتوعيتهم بالظاهرة، والاستماع إلى تجاربهم، والعمل المشترك لفضح من يمارسها من خلال تأسيس مواقع خاصة لذلك، والإبلاغ عمن يمكن التعرف على شخصيته، نيابة عن الضحية وبتوكيل منها، حتى يتم الحفاظ على سرية شخصيتها بما لا يعرضها لأي أذى على المستوي الاجتماعي.
- في مجال البحث عن آليات التعامل يلزم التركيز علي في البداية على المواجهة المجتمعية من خلال وضع برامج توعية للضحايا المحتملين من جانب، ومحاولة تقويم الجاني المفترض من جنب آخر. على أن يسير ذلك جنباً إلى جنب مع المواجهة القانونية للحالات التي يمكن فيها التوصل إلى الجاني، وايقاع العقاب الرادع عليه بما يؤدى إلى الحد من هذه الممارسات الآثمة. وفي هذا الخصوص يلزم تدشين حملة إعلامية من قبل الجهات الرسمية المتخصصة (مجالس المرأة، ومجالس حقوق الإنسان)

للتوعية بما تتضمنه القوانين من عقوبات على مثل هذه الجرائم وطرق الإبلاغ عنها، مع تقديم كافة سبل المساعدة اللازمة للحفاظ على سرية شخصية الضحية.

- تشجيع الاتجاه الذاهب إلى فتح صفحات على مواقع التواصل الاجتماعي تقوم من خلاله النساء والفتيات بنشر كل ما قد يتوفر لديهم من معلومات عن المتحرشين ومحتوى رسائلهم، ومن الأمثلة العملية على ذلك صفحات من قبيل: "لا للتحرش"، "شفت تحرش"، "العربي المريض".

- التشجيع على استخدام اعدادات إليكترونية تحقق أعلى مستوي من الخصوصية على شبكة الإنترنيت تضمن تحقيق أعلى مستوي من الخصوصية والحد من الاتصالات غير المرغوب فيها، مع وضع نظام فلتر جيد للبريد الإليكتروني يضمن تحول الرسائل أو الكلمات البذيئة إلى قامة الرسائل غير المرغوب فيها أو المجهولة المصدر.

قائمة المراجع

أولاً-الكتب

- د. أحمد عوض بلال، مبادئ قانون العقوبات المصري: القسم العام، دار النهضة العربية، القاهرة، مصر، 1999.
- د. أحمد شوقي أبو خطوة، شرح الأحكام العامة لقانون العقوبات، دار النهضة العربية، مصر، القاهرة، 2000.
- د. أحمد فتحي سرور، الوسيط في قانون العقوبات: القسم العام (قانون العقوبات ونطاق تطبيقه- التجريم والإباحة- الجريمة- المجرم- العقوبة) مطورة ومحدثة، دار الأهرام للنشر التوزيع والإصدارات القانونية، الطبعة السادسة، القاهرة، مصر، 2014.
- اللواء د. فؤاد جمال، الجرائم المعلوماتية، دار النشر الحديثة، مصر، 2011.
- د. محمود نجيب حسنى، "علاقة السببية في قانون العقوبات"، طبعة نادي القضاة، مصر 1984.
- د. محمود نجيب حسن، قانون العقوبات: القسم العام، دار النهضة العربية، مصر، 1998.

ثانياً- الدراسات والمقالات

- تامر البطراوي، "ظاهرة التحرش: تحليل سيكولوجي سوسيولوجي، موقع شبكة الحوار المتمدن، 16 مارس 2018، الرابط:

https://www.ahewar.org/debat/show.art.asp?aid=592462

- د. ثناء هاشم محمد، "واقع ظاهرة التنمر الإليكتروني لدي طلاب المرحلة الثانوية في محافظة الفيوم وسبل مواجهتها: دراسة ميدانية"، مجلة جامعة الفيوم للعلوم والتربية النفسية، العدد الثاني عشر، الجزء الثاني، مصر، .2019.
- روعة نضال الشقران، التنمر الإليكتروني وآثاره القانونية والاجتماعية، وكالة أنباء عمون، الأردن، 15 أكتوبر 2020.

https://www.ammonnews.net/article/568376

- عالية الشريف، "ارتفاع التحرش الإليكتروني عند الشباب بنسبة 70%"، جريدة الوطن السعودية، 25 مارس 2016.

https://www.alwatan.com.sa/article/295316

- عمرو عبد العاطي، "التحرش الاليكتروني من الشارع إلى شبكات التواصل الاجتماعي"، 2015/4/28.

https://mustaqila.com

- محمد حسون، "التنمر الإليكتروني بين الأسباب والعلاج، موقع العطاء الرقمي، الرابط:

https://attaa.sa/library/view/385

- د. محمود سيد أحمد عبد القادر عامر، إشكالية تحديد المسئولية الجنائية للتحرش الإليكتروني كجريمة اليكترونية والجهود الدولية لمكافحته، مجلة الدراسات القانونية والاجتماعية، جامعة مدينة لسادات، مصر، المجلد (7)، العدد (1) 2021.
- محمود عبد العظيم محمد سليمان، "التحرش الجنسي الإليكتروني: دراسة في الأنماط والدوافع"، شبكة النبأ المعلوماتية، 11 ديسمبر 2018، الرابط:

https://annabaa.org/arabic/studies/13835

- كلير ماكفيير، "التنمر الإليكتروني: ما هو وكيف يمكن إيقافه"، موقع منظمة الأمم المتحدة للطفل، اليونيسيف، 11 فبراير 2020، الرابط:

https://www.unicef.org/jordan/ar

ثالثاً- كتيبات

- "قل لا ... للتنمر الإليكتروني: أحمي نفسك من التنمر الإلكتروني... وساهم في حماية الآخرين". كتيب صادر عن هيئة تنظيم الاتصالات، جمعية البحرين النسائية، مملكة البحرين، بدون تاريخ، الرابط:

https://bahrainws.org/

المؤتمر العلمي الدولي تحت عنوان:

الأمن السيبراني في تشريعات الدول العربية

المنعقد يومي: الجمعة والسبت 16 و17 يوليوز 2021
بنادي المحامين تاركة مراكش